SEGURIDAD EN SERVIDORES LINUX



#22

WIRELESS PRESENTE Y FUTURO

¿Moda...
VIRTUALIZACION
...o innovación estratégica?

Tecnologías detrás de
BLACKBERRY

Wireless MESH NETWORKING
IEEE 802.11s

VoIP Open Source
ASTERISK

INNOVADORES IT



APRENDA CON LOS MEJORES
Disaster Recovery Planning (DRP), Paul D´Jallad Baña CTO, Aon Risk Services Latin America.

Network
STORAGE

WWW.NEXWEB.COM.AR
ISSN 1668-5423
9 771668 542003 00022
Dist. Cap.: Vaccaro Sanchez y Cía. S.C. - Interior: DGP
Correo Argentino FRANQUEO A PAGAR Cta. 16185

Asistencia Técnica Profesional y a Escala

- Atención, Consolidación y Roll Out de Sucursales a Nivel Regional
- Obras de Infraestructura Vinculadas a la IT (en todos los rangos de complejidad).
- Networking. Provisión, Montaje y Configuración de Redes Inalámbricas Multi Marca (Co., Soho, Etc.)
- Soluciones Wi Fi de Alta Seguridad
- Servicio Oficial para Grupos de Afinidad (Clientes Banco Río, Clientes Uol, Otros.) ■
- Instalación Masiva de Internet
- Exclusivo Software (propietario) para el Seguimiento de Servicios
- Cursados (SupportStepSystem) Integración

■ **Solicite Condiciones para su Entidad.**



- Mesa de Ayuda Telefónica "Help Desk"
- Atención en Domicilio "Soporte On Site"
- Reparaciones en Laboratorio "Break & Fix"
- Instalación y Mantenimiento de Servidores
- Administración de Garantías
- Mudanzas "Llave en Mano"
- Seguridad Lógica (Antivirus, Antispam, AntiHacker, Etc.)
- Provisión de Partes y Componentes
- Upgrade Masivo de Hard y Soft
- Capacitación
- Consultoría
- Eventos
- Guardia 24 Hs.

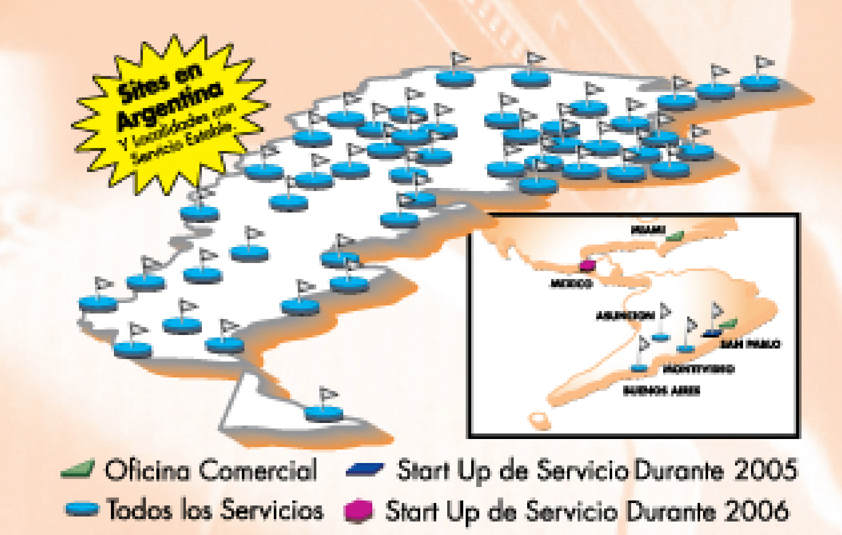
El Mundo del Soporte

A Member of SupportLand Network

Participe en Negocios Corporativos, Sin Costo de Ingreso al Sistema.

Si Usted Posee una Estructura de Sistemas, Local/es o es Profesional Autónomo del Área (No Excluyente por Dimensión), Forme Parte de la Única Red de Soporte Técnico Independiente de la Región en Calidad de AGENTE TÉCNICO OFICIAL, Beneficiándose de una Imagen, Publicidad y Sistemas Unificados. Métodos Preestudiados en Constante Actualización y Background Tecnológico de Última Generación.





Organización Mundo del Soporte Latin América

Show Room & Main Call Center: Edificio Torre Humboldt 2495 7º Piso (Esq. Santa Fe)
(C1425FUG) Palermo - Ciudad Autónoma de Buenos Aires - Argentina
Sucursales y Red de Agentes Oficiales en toda la Región - **Tel.: (54-11) 5252-7500 / 5238-0300**

www.mundodelsoporte.com



DIRECTOR
- Dr. Carlos Osvaldo Rodriguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

COORDINADOR EDITORIAL
- Carlos Rodríguez Bontempi

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

DIRECTOR COMERCIAL
- Ulises Román Mauro
umauro@nexweb.com.ar

EDITORES
- Carlos Vaughn O'Connor
- Carlos Rodríguez

EDITOR TÉCNICO
- Alejandro Cynowicz
redeccion@nexweb.com.ar

DISTRIBUCIÓN
- Mariano H. Agüero
distribucion@nexweb.com.ar

SUSCRIPCIONES
- Maximiliano Sala
- Martín Guaglianone
- Andrés Vázquez
suscripciones@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- DCV Esteban Báez
- Carlos Rodríguez Bontempi

PREIMPRESIÓN E IMPRESIÓN
IPESA Magallanes 1315. Cap. Fed.
Tel 4303-2305/10

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Vaccaro, Sánchez y Cia. S. C. Moreno 794, Piso 9. C1091AAP- Capital Federal Argentina.
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1
C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Si desea escribir para nosotros, enviar un e-mail a: articulos@nexweb.com.ar





Nota del Editor

Si hay algo que nunca falta en el mundo IT son las "Buzzwords".

Pero antes de ver cuáles circulan en IT hoy, entendamos lo que son las Buzzword.

De wikipedia: un "Buzzword" (también conocida como "palabra de moda" o "palabra en boga") es una expresión, muchas veces un neologismo (palabra recientemente creada o acuñada), usada comúnmente en entornos de ejecutivos, técnicos y a veces políticos. Las buzzwords se transforman en ubicuas pero su significado exacto es muchas veces poco claro. Muchas veces el "furor" que rodea a las nuevas tecnologías transforma términos técnicos en buzzwords.

Y es exactamente así en IT.

Algunos de los buzzwords que se escuchan hoy en IT son: "Consolidación de servidores", "Virtualización", "DRP, Disaster Recovery Planning, "CISSP", 802.11 en general y 802.11s relacionada Wireless Mesh Networking, "Consumer Electronics", "SOA (Service Oriented Arquitectures)", "Wi-fi", "WiMax", "ZigBee", "SOX (Sarbanes Oxley)","HIPAA", "ITIL", "Social bookmarking", "OPML", "RSS feeds" entre otras.

Quien lee NEX IT Specialist, es o se está preparando para ser un especialista/experto que sabe que encontrará en la revista una respuesta a qué es cada uno de estos buzzwords. Como se desprende de la definición, nuevas tecnologías y buzzwords son casi la misma cosa. En particular, si esas tecnologías han tenido gran repercusión. Y NEX es justamente la conjunción de ambos-: "Tecnología para Expertos".

Por otro lado, en el ambiente Microsoft, el término "Trustworthy Computing" ha sido un buzzword ligado a la seguridad. Hoy es la palabra "community" la que flota en el aire en Microsoft y en sus acciones. Vean por ejemplo el esfuerzo a través de Robert Rebholz y TWN (www.thenetworkingnetwork.com o http://channel9.msdn.com/Showpost.aspx?postid=134574) donde la idea es promover redes confiables de profesionales IT. Ejemplo de ésto en el ámbito de Latinoamérica son: el proyecto educativo ALSI (Academia Latino Americana de Seguridad Informática), Technet con sus webcasts y learning center, MSDN 5 Estrellas, apoyo a grupos como "desarrollador@s", "MS jóvenes" y muchas otras acciones.

Una comunidad se forma con gente que habla el mismo lenguaje y que busca encontrar sus pares (peers) para resolver problemas comunes. Se crean newsgroups, blogs, publicaciones y grupos de usuarios, básicamente buscando ayudarse unos a otros.

Y justamente, una comunidad es lo que se está creando alrededor de NEX IT Specialist. Ésto es algo que estamos constantemente promocionando y nos enorgullece. Por ejemplo, este mes inauguramos nuestro newsletter mensual para suscriptores, realizaremos nuestro primer estudio sobre el perfil del profesional de IT y networking en Argentina, buscamos junto a los vendors la promoción de cursos de capacitación (ver detalle del sorteo de un curso RHCE en la publicidad conjunta con Red-Hat), desde febrero 2006 iniciaremos un ciclo de charlas especializadas en seguridad informática. Y esperamos seguir brindando más a esta comunidad.

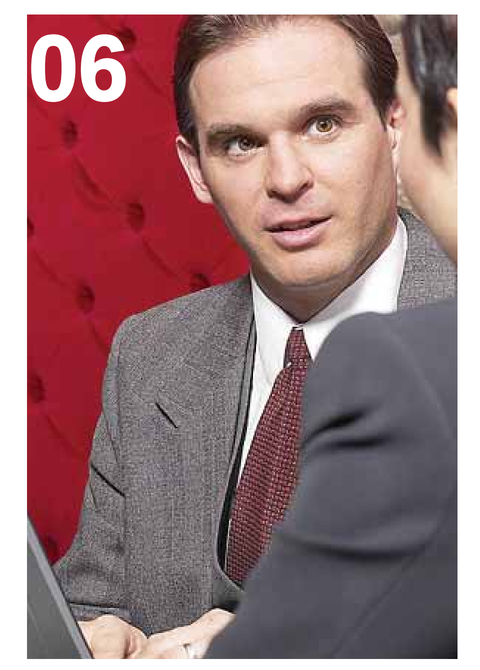
Finalmente, les anunciamos que a partir de este número comenzaremos la serie "Seguridad en Linux: de 0 a 100 en 5 notas". Su autor, Luis Otegui las ha redactado de modo de conformar un bloque, aunque cada presentación conservará su individualidad; Parte desde las consideraciones que hay que tener a la hora de instalar el sistema operativo (primera nota), e irá evolucionando a través de los siguientes temas en las notas siguientes:

- Firewalls en hosts y su interacción con otros hosts. Firewalls de borde.

Análisis de logs.

- Planteo de modelo de seguridad en una red. Segmentación. Sistemas de detección de intrusos. Control de tráfico.
- Auditorías de seguridad. Prácticas sistemáticas de seguridad.
- Cómo lidiar con una intrusión. Contención de daños. Análisis forense.

Si quiere estar al tanto de todo lo nuevo: continúe leyendo este ejemplar.



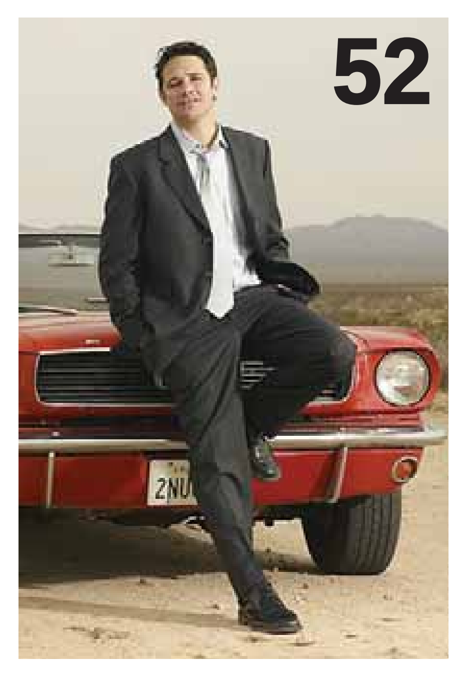
Disaster Recovery Planning

Luego del 9/11, los planes de recupero ante desastres, dejaron de ser artículos de lujo para convertirse en una necesidad. Las organizaciones comenzaron a recibir presiones internas y externas para desarrollar planes con el objetivo de proteger sus activos.



Wireless, Presente y Futuro

En este artículo, describiremos las tecnologías inalámbricas que están desplazando a las líneas cableadas, como a su vez los pros y contras de sus respectivos protocolos. Desde tecnologías pioneras a vanguardistas, analizaremos WiFI, WiMAX, y ZigBee.



Seguridad en Linux Nota 1

... había un disco rígido, vacío -o quizá con otro sistema operativo viviendo en él. Luego, decidimos instalar Linux, y convertirnos en un deus in machina, el súper usuario, root. Y, a partir de ese momento, comenzamos con un camino que puede ser tan tortuoso -y tan interesante- como nosotros queramos.



Firma Digital

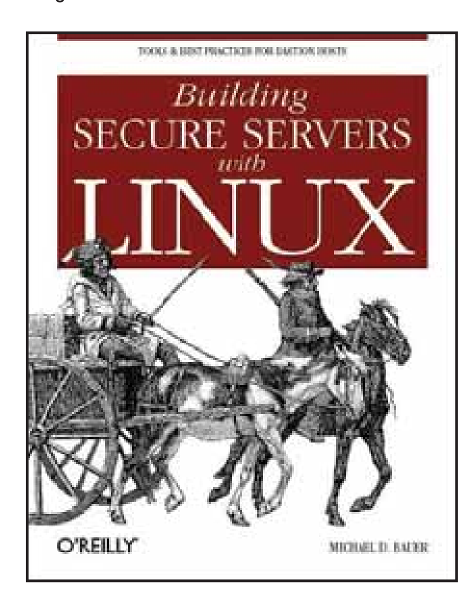
Es un tipo de método de autenticación para información digital, análoga a las firmas físicas comunes realizadas en papel. Su implementación se realiza usando técnicas del campo de la criptografía de llave pública.

SUMARIO

LIBRO LINUX

"Building Secure Servers with LINUX"
Autor: *Mick Bauer,*
Editorial: *O´Reilly, 2005.*
ISBN: *0596002173*
(Existe versión en español publicado por Editorial Anaya Multimedia, año 2005 (ISBN: 8441518777)

Existen muchos libros de seguridad de servidores Linux. En éste, Mick Bauer nos presenta un excelente libro que nos complace recomendar.
Mick es Editor de Seguridad de la prestigiosa revista Linux Journal (www.linuxjournal.com) y durante muchos años mantuvo la prestigiosa columna "The Paranoid Penguin". Entre sus credenciales Mick tiene la prestigiosa certificación CISSP del ISC2 (www.isc2.com).
Destacar la importancia de Linux en el mundo de servidores hoy es redundante. Destacar la importancia de mantenerlos seguros también.
Mick trata en forma precisa y clara temas como: Seguridad de base de datos centrada en MySQL, Diseño de perímetros de red, Autentificación mediante OpenLDAP, Introducción al cifrado de correo electrónico, el agente de servicio de correo Cyrus IMAP, Gestión y monitorización del System Log, el servidor de FfP vsftpd, y DNS seguros, entre otros.
"Building Secure Servers with LINUX", se ubica en el 1° puesto del ranking de los libros más comprados en Amazon.com cuando hacemos un search con "linux security".
Afortunadamente la editorial Anaya publicó el libro con una buena traducción a nuestro idioma (que no es siempre el caso). El libro puede ser adquirido en la librería Cúspide (www.cuspide.com) por U$S 44,00 = $ 134,50, bajo el título "Seguridad en servidores Linux".



CALENDARIO DE EVENTOS IT EN ARGENTINA PARA EL 2006		
Fecha	**MARZO**	**Informes**
15	**Segurinfo 2006 -** Sheraton Libertador.	www.segurinfo.org.ar
	ABRIL	
	Jornadas Trabajo IT - Sheraton Buenos Aires	www.worktec.com.ar - info@worktec.com.ar Tel.:4511.3300
	JUNIO	
8	**Jornadas Trabajo IT Córdoba -** Córdoba Capital.	www.worktec.com.ar info@worktec.com.ar Tel.:4511.3300
9	**CIASFI Córdoba -** Córdoba Capital.	
22	**1er Jornada Nacional de Calidad en Software -** Sheraton Libertador.	
	SEPTIEMBRE	
19 y 20	**Consecri-Consetic 2006 -** Sheraton Libertador.	www.worktec.com.ar - info@worktec.com.ar Tel.:4511.3300
	OCTUBRE	
3 al 6	**EXPO COMM -** La Rural, Predio Ferial de Buenos Aires.	www.expocomm.com.ar
6 y 7	**2do Congreso Nacional de Estudiantes de Sistemas y Tecnología de la Información. -** Lugar a confirmar.	www.worktec.com.ar - info@worktec.com.ar Tel.:4511.3300
	NOVIEMBRE	
2 al 5	**AES - Argentina Electronic Show -** La Rural, Predio Ferial de Buenos Aires.	http://www.aeshow.com.ar/es_services_contact_us
19 y 20	**Jornadas Trabajo IT 2 -** Sheraton Libertador.	www.worktec.com.ar - info@worktec.com.ar Tel.:4511.3300

Si desea ver su evento IT publicado en esta sección, por favor háganos llegar la información respectiva a: eventos@nexweb.com.ar

Disaster
Recovery
Planning

DRP ¿LUJO O NECESIDAD?

Paul D´Jallad Baña
Chief Technology Officer, Aon Risk Services Latin America

Luego del 9/11, los planes de recupero ante desastres, dejaron de ser artículos de lujo para convertirse en una necesidad. Las organizaciones comenzaron a recibir presiones internas y externas para desarrollar planes con el objetivo de proteger sus activos.

Cuando me reuní con los amigos de NEX IT para comentar los objetivos y alcances de esta nota, coincidimos rápidamente en que lo que queríamos transmitir y compartir era una experiencia con fuerte contenido técnico sobre el planeamiento de recupero ante desastres o DRP.

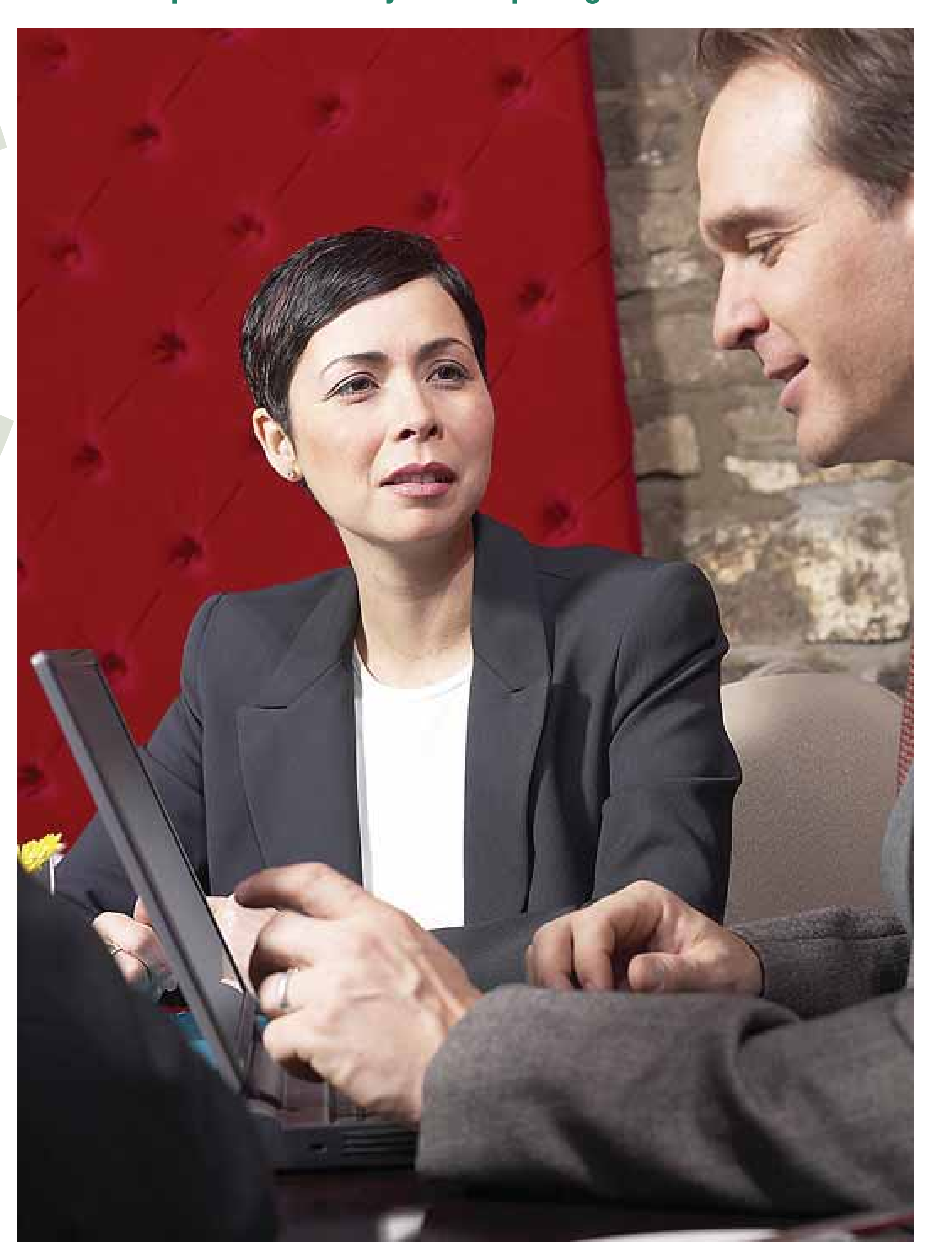
Luego de recorrer más de 32 ciudades en el planeta, tanto en América como en Europa, trabajando con diferentes empresas, he comprobado que el concepto de DRP es algo que todavía no está en la cultura de muchos países, especialmente en la Argentina. Estamos frente a un tema que no es una moda pasajera, es un tema que está entre nosotros mucho antes que los ataques al WTC, Londres, Madrid y los desastres climáticos que nos han estado afectando en los últimos años. Es un nuevo condimento que estará presente en nuestros proyectos de infraestructura tecnológica, desarrollo e implementación de aplicaciones, mantenimiento de nuestros servicios de IT, y nuestros budgets.

En la organización para la cual trabajo hemos podido implementar con éxito una única solución de DRP regional que cubre las necesidades corporativas y las necesidades propias de cada uno de los países de Latinoamérica y Caribe. En esta nota iremos recorriendo juntos los diferentes aspectos de esta solución.

Un poco de teoría…

El **DRP** o **D**isaster **R**ecovery **P**lanning, **es uno de los componentes del llamado Enterprise Recovery Planning (ERP)**. Este planeamiento incluye a todos los sectores críticos de la empresa, como ser la alta dirección, gerencias, jefaturas y áreas operativas o de servicio, y también entidades externas a la empresa como los principales proveedores y consultores.

Todas las empresas, grandes, medianas o pequeñas (The Size doesn´t matter…) se han convertido en IT dependientes. Ésto determina que las áreas de tecnología sean un partícipe de vital importancia en este planeamiento.



Clase	Eventos	Causas Probables o Posibles
Interrupción	Rotura o Desperfectos Menores	Hardware, Infraestructura
	Inoperabilidad de software	Caída, bloqueo accidental o intencional del software.
	Indisponibilidad de RR.HH.	Ausencia de personal clave
	Indisponibilidad de conectividad	Caída de enlaces, indisponibilidad de conexión a Internet.
	Indisponibilidad de proveedores.	Corte prolongado de energía eléctrica
	Destrucción física parcial	Accidente, incendio localizado, robo, sabotaje.
	Destrucción física total	Incendio grave, atentado, catástrofe natural.
Inaccesibilidad	Imposibilidad de acceso Temporal	Huelga, desorden civil.
	Imposibilidad de acceso Prolongada	Inundación, motín, sedición, desórdenes políticos.

Cuadro1

El objetivo que persigue todo ERP es el de asegurar la continuidad del negocio, la atención de los clientes y activos de la empresa ante desastres, crisis o emergencias.
Como se aprecia en el grafico debajo, al tope de la pirámide se encuentra el panel de control de todo ERP, que es la **Gestión** de las crisis.
El objetivo de este componente es el de identificar lo más rápido posible un incidente, analizar su impacto o riesgo, responder de manera efectiva a las emergencias, y la administración general de la recuperación y estabilización de la organización ante incidentes.

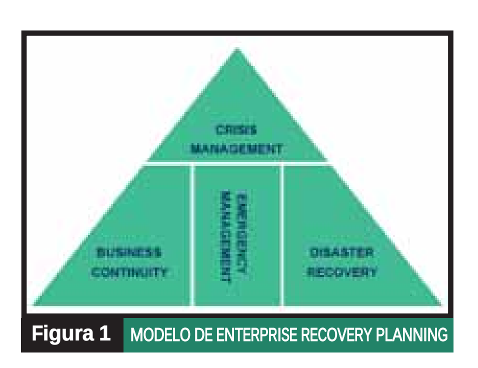


Figura 1 MODELO DE ENTERPRISE RECOVERY PLANNING

Es muy común contar con varias de estas pirámides, de acuerdo a la magnitud de la operación o a la distribución geográfica de las oficinas. Este concepto del ámbito empresarial se ha "copiado" de las prácticas militares y de defensa, donde la administración y gestión de crisis es moneda corriente. De esta manera, cuando ocurre un incidente en una oficina satélite, los distintos equipos de gestión de crisis se sincronizan y actúan en conjunto. Otro motivo por el cual siempre existen componentes redundantes en este esquema, es la posibilidad de que el equipo local de administración de crisis haya sido afectado por la misma crisis y se encuentre desarticulado / inoperativo. Cabe mencionar que esto sucedió en catástrofes recientes como el Tsunami que azotó Asia y el Pacífico y Katrina en USA.
El **Business Comtinuity Planning** o BCP, tiene como finalidad determinar las prioridades de recupero ante desastres y el desarrollo de planes para la continuidad de los procesos de negocio vitales de la empresa. Básicamente, el BCP define que aplicativos y servicios deberán ser recuperados y en qué orden, así como la definición de los procesos de negocio ante una crisis.
El DRP desarrollará planes para recuperar la infraestructura de IT, así como los aplicativos y servicios de tecnología que el negocio necesita para su operación.
Antes de entrar en detalle, quiero aclarar que tener una correcta estrategia de backup, ejecutar los backups todos los días, tener una correcta estrategia para control y mitigación de virus informático, no significa que tenemos un plan de recupero ante desastres.
Un punto interesante es la relación entre el BCP y el DRP. Mientras el BCP define las prioridades de recupero para el negocio, el DRP es el encargado de -en base a este input- recuperar la infraestructura informática, aplicativos y servicios. El **BCP** es quien dicta **qué y cuándo** recuperar los componentes de IT y el **DRP** es el encargado del **cómo**.

Emergencias versus Crisis

Hemos hablado de emergencias y crisis. Veámoslas un poco más en detalle.
Una emergencia es administrada por la oficina, empresa o sucursal afectada principalmente por la misma, y tiene las siguientes características:
-Puede ser manejada a nivel local y no necesariamente expandirse a otras oficinas.
-No tiene un impacto financiero significativo.
-No hay un riesgo potencial de lesión o muerte de personas.
-No afectarán de manera negativa la imagen de la empresa con clientes, proveedores o el mercado financiero.
-No genera mucho interés en la prensa.
Podemos citar como emergencias los siguientes ejemplos:
Imposibilidad de acceder a las facilidades de la oficina por:
-Piqueteros.
-Cortes de suministro eléctrico.
-Incendio en la cercanía de la oficina.
Imposibilidad de operar los servicios y aplicativos en la oficina por:
-Evacuación de edifico planificada.
-Cortes de suministro eléctrico.
-Caída de enlaces o servicios por parte de proveedores.
-Etc.
Una crisis sin embargo, requiere que se dispare una alerta a los distintos equipos de administración de crisis. Una crisis, es definida como un evento que ha causado lesiones o muertes y/o potenciales pérdidas financieras, exposición jurídica o en los medios.
Un evento como el mencionado arriba contiene uno o más de los siguientes componentes:
Vida Humana
-Involucra lesiones severas o muerte de empleados / terceros.
-Involucra amenaza a empleados o terceros.
Operaciones Corporativas
-Serias amenazas a la continuidad de las operaciones de la empresa por daños.
-Afecta parcial o totalmente la oficina y sus alrededores.
Finanzas Corporativas
-Pérdida de clientes por causa de la crisis.



-Pérdidas económicas que afectan directamente el ingreso operativo neto de la empresa.

Imagen Corporativa

-Impacto en la credibilidad con clientes, socios y proveedores.

-Impacto negativo en los mercados financieros y de acciones.

-Atractivo para los medios de comunicación masivos.

¿Qué hay de nuevo, viejo?

No hace muchos años la Capital Federal quedó sin suministro eléctrico en 12 barrios incluyendo zonas como el microcentro, durante 5 días.

Cortes masivos de electricidad…ummm, veamos cosas que ocurren más a menudo ¿Cuántas veces no pudieron entrar a la oficina por manifestaciones en las calles de Buenos Aires? (piqueteros, huelgas, etc.)

Sigamos con este ejercicio de "drill down": ¿Cuántas veces un componente crítico de un servidor se rompió y hubo que cambiarlo por uno nuevo? ¿Cuántas veces se cayó un enlace con una oficina satélite provocando que la misma quedara completamente aislada?

¿Cuántas veces hubo que enviar e-mails desde el área de sistemas informando a toda la empresa que por "razones técnicas" hay que "bajar" el aplicativo ABC?

Sin lugar a dudas, lo que estoy mencionando no son crisis como la devastación provocada por un huracán, la caída de rascacielos o inundaciones provocadas por tsunamis, pero tienen las mismas consecuencias: dejar sin servicio parcial o total de IT por un tiempo determinado a la organización. ESE tiempo, el esfuerzo (tanto humano como económico) y CU{aNDO es que se presenta el problema, son las variables que determinan el tamaño



Escenario	Situación
Escenario 1	**Inoperabilidad de software.** Uno o más servicios se hallan interrumpidos pero el resto de los sistemas funciona satisfactoriamente
Escenario 2	**Inoperabilidad de hardware.** Uno o más servicios se hallan interrumpidos pero el resto de los sistemas funciona satisfactoriamente.
Escenario 3	Una o más personas-clave del personal de IT no se encuentran disponibles. La prestación de los servicios dependientes de dichas personas puede estar comprometido.
Escenario 4	Se ha interrumpido la conectividad con el backbone de la red, o el acceso a Internet. Los servicios locales funcionan satisfactoriamente pero la conexión con el exterior se halla total o parcialmente interrumpida.
Escenario 5	El Data Center se encuentra total o parcialmente en imposibilidad de operar o existe amenaza de que quede en imposibilidad de operar antes de transcurridas X horas debido a que uno o varios proveedores externos han interrumpido sus prestaciones.
Escenario 6	Destrucción física parcial del Data Center. Algunos servicios están disponibles, o pueden ser recuperados, pero los dependientes del material destruido se encuentran interrumpidos.
Escenario 7	Destrucción total del Data Center. No hay servicios disponibles ni posibilidades de restaurar el Data Center localmente en menos de X días.
Escenario 8	El acceso al Data Center se encuentra impedido y la situación se mantendrá por un lapso previsible no mayor a X días corridos. Los servicios del Data Center han quedado en funcionamiento pero es imposible acceder físicamente al mismo.
Escenario 9	El acceso al Data Center se encuentra impedido y la situación se mantendrá por un lapso previsiblemente mayor a X días corridos. Los servicios del Data Center han quedado en funcionamiento pero es de prever que irán cayendo poco a poco debido a que no se tiene acceso físico a las instalaciones.

Cuadro 2

del incidente. Obviamente que ante mayor escala de crisis, mayor probabilidad de que el tiempo fuera de servicio sea mas prolongado. Vale decir que diariamente estamos bajo situaciones de DRP, en diferentes escalas o escenarios; veamos algunos ejemplos:

Vamos a comenzar analizando las posibles situaciones básicas, que son interrupción e inaccesibilidad (Cuadro1). Veamos ahora algunos escenarios posibles (Cuadro 2).

Nos podemos dar cuenta que en nuestras operatorias diarias de IT, lidiamos con escenarios del 1 al 4. Comenzando con el escenario 5 es cuando comenzamos a tratar con una emergencia o crisis, donde el peor escenario es el numero 9.

Vemos que en la tabla mencionamos XX días o XX horas. ¿Quién es el encargado de determinar esos números? Ésto surge del análisis, estudio y trabajo conjunto de las áreas de negocio, IT y principales proveedores. Básicamente se establecen los RTO y RPO. El **RTO** o **Recovery Time Objectives** establece cuán rápido podemos recuperarnos de un desastre, mientras que el **RPO** o **Recovery Point Objectives**, define cuánto estamos dispuesto a perder en caso de un desastre. En lo personal reemplazaría RTO por "downtime" o "tiempos de caída" y al RPO por "pérdida de datos" o "loss of data".

Presiones internas y externas

Al comienzo de la nota mencioné el tema de las presiones internas y externas que reciben las empresas con respecto a DRP. Podemos enumerar algunas presiones internas:

- Comité de Dirección.
- Auditorias internas.
- Normas y procedimientos internos de la empresa.
- Accionistas.

Pero también hay presiones y demandas externas, las cuales son sumamente importantes

- Demanda de clientes.
- Legislación.

Veamos esta última. En lo que respecta a legislación, en las grandes corporaciones, existe la llamada ley de **Sarbanes Oxley** o **SOX**. Básicamente, y para no entrar en detalles, SOX se ocupa de hacer que los directivos de las organizaciones tengan una gestión o conducta transparente y auditable, así como presionar sobre la forma de trabajo de las auditorías independientes.

Hay muchas discusiones acerca de si SOX aplica en casos de desastre o crisis. Sin embargo, SOX exige que la organización debe de ser capaz de proveer cualquier tipo de información, sin importar en que medio de almacenamiento se encuentre.

Desde el punto de vista de IT, tenemos que ser capaces de brindar cualquier tipo de información en formato digital (almacenada en discos, cintas, etc.) en el momento que se requiera, no importa si estamos en emergencia o en el desarrollo normal del negocio.

DRP Oriented…

Vemos entonces que DRP es mucho más que una lista de tareas y una planilla con los contactos a llamar en caso de una emergencia. DRP es una forma de trabajo, es una manera de operar y de hacer negocios, es una variable más a tener en cuenta con cada proyecto de IT.

Ahora no sólo basta con hacer un buen sizing de infraestructura para la implementación de un centro de cómputos o la implementación de un aplicativo. Cada componente de IT que incluimos en nuestra operatoria, deberá pasar la pregunta de ¿Este componente es crítico para la continuidad del negocio ante una crisis o emergencia? Si la respuesta es sí, entonces debe ser incluido en nuestro plan de DRP. Esto es trabajar con mentalidad DRP Oriented.

Desarrollando una estrategia de DRP

Ya hemos visto bastante teoría, veamos cómo desarrollamos una estrategia de DRP.

AON
CORPORATION

Con su casa matriz en Chicago, Aon Corporation es proveedor líder de servicios de administración de riesgo, seguros, capital humano y administración de consultoría.

Una ventaja clave es su amplitud de visión de la industria de los seguros. Con una plantilla de empleados de 47000 personas trabajando en 500 oficinas en más de 120 países, pueden anticipar como cambios en un sector pueden impactar en otro; Ésto gracias a la integración de sus servicios y su experiencia en centenares de disciplinas alrededor del mundo.

Dado que DRP es uno de los componentes del plan integral de recuperación ante desastres, nos concentraremos en aquellas areas del DRP que tengan que ver directamente con IT. Por la extensión y complejidad, dejaré fuera del alcance de esta nota componentes como análisis de riesgos operativos, financieros y de pérdida de beneficio. Éstos son componentes muy importantes en todo plan de DRP y aconsejo lecturas que permitan profundizar en estos tópicos.

Al confeccionar un DRP, tenemos que tener en cuenta las siguientes premisas:

- Mitigación.
- Alistamiento.
- Reacción.
- Recuperación.

La primera fase es la de mitigacion. Aquí es donde nos concentramos en minimizar la posibilidad de que ocurra un desastre, así como de reducir los efectos negativos ante la ocurrencia de un desastre.

Un buen ejemplo de esto es el de realizar testeos de penetración en nuestras redes informáticas, simulando ataques externos e internos. Otro ejemplo es el de verificar el correcto mantenimiento de los diferentes componentes de seguridad de un centro de cómputos, como ser sistemas de acceso y sistemas de control y extinción de incendios.

En la etapa de alistamiento, es donde trabajamos en conjunto con el **BCP**, juntando información de nuestros aplicativos, redes, infraestructuras, servidores, etc. En esta etapa trabajamos con planillas de análisis de impacto al negocio (**BIA**), para determinar qué tiene que ser recuperado ante un desastre y en qué orden.

En la etapa de reacción, es donde en base a una evaluación de desastre, decidimos qué tipo de reacción o respuesta dispararemos. Es muy diferente una respuesta ante una pérdida de agua próxima a un centro de cómputos que la rotura parcial o total de un servidor crítico.

Por último, tenemos la etapa de recuperación propiamente dicha. Aquí es donde se establecen las tareas y actividades específicas a realizar para volver a estar operativos frente a un desastre.

¿Por dónde empezamos? Como todo proyecto, lo aconsejable es comenzar con una reunión de *kickoff*, para presentar y discutir los siguientes temas:

- Identificar los componentes que estarán "in scope" del plan de DRP. Los principales componentes son siempre los Data Centers. también pueden incluirse software de las estaciones de trabajo, componentes de IT en ubicaciones remotas, etc.
- Como todo proyecto debemos tener un responsable del proyecto. Ésto depende de la cultura y la magnitud de la organización. Podemos necesitar más de un gerente de proyecto y comités de decisión y dirección.

Generalmente el gerente de proyecto de DRP es una persona del área de tecnología, pero también puede ser un consultor externo o un miembro del pool del equipo de project managers de la empresa.

- Definición de los roles y responsabilidades de los participantes. Como en todo proyecto de IT, es fundamental el respaldo y compromiso de las



más altas áreas de dirección.
- Acordar sobre los próximos pasos a realizar en la confección del plan de trabajo y fechas previstas para los entregables y reuniones de comunicación y dirección.

A ponerse a trabajar...

No se asusten, la mayoría de la información necesaria para desarrollar una solución de DRP no la tenemos que comenzar a trabajar desde cero, gran parte de esta información ya existe en los diferentes sectores de IT de nuestras empresas.

Seguridad Física

Lo primero que tenemos que documentar y analizar es la seguridad física de los componentes de IT. Qué tan seguros están nuestros servers, Data Centers y demás componentes core.
- ¿Quiénes están autorizados a acceder a los Data Centers y cuándo?
- ¿Las consolas de los servidores tienen políticas de auto bloqueo cuando están desatendidas?
- ¿Contamos con detectores de humo y calor? ¿Están con el mantenimiento adecuado?
- ¿Existen en los Data Centers materiales inflamables como cajas de plástico o de cartón? ¿Cuántas veces hemos visto cajas de cartón de embalaje de servers, routers, etc. en los Data Centers?

Seguridad de las redes

El próximo paso es documentar la seguridad y vulnerabilidad de nuestra red informática. A ningún encargado de Data Centers le gusta reconocer que sus sistemas y redes son vulnerables. Aquí lo importante es dejar en claro que no se estará "acusando" a una o más personas, sino que es necesario identificar posibles fallas que deriven en una situación de DRP.
Algunos de los temas para analizar cuando veamos las seguridades de las redes:
- ¿Contamos con documentos y procedimientos en el área de seguridad informática?
- ¿Se mantienen actualizados esos documentos y procedimientos?
- ¿Están agendados en el plan de sistemas tests de penetración?
- ¿Los planes y procedimientos son comunicados correctamente?
- ¿Los logs de los Firewalls son revisados de acuerdo a una política establecida?
- Ser honestos y documentar cuáles son nuestras vulnerabilidades.
- Analizar que riesgos se pueden desprender de estas vulnerabilidades.
- Trabajar sobre esos riesgos para mitigarlos.

Servicios Críticos

Cuando hablamos de servicios críticos, básicamente nos referimos a los servicios que son vitales para la operación de nuestra empresa. Aquí no hay que hacer un estudio minucioso de los servicios que necesitamos sino sólo de los más críticos. Podemos citar como primer ejemplo las comunicaciones. Cada vez son más los negocios y operaciones que están basados en Internet y enlaces a sucursales o redes corporativas.
Con respecto a las comunicaciones, debemos de documentar qué tipo de conexiones realmente necesitaríamos en caso de emergencia para poder determinar si necesitamos vínculos redundantes, rutas o redes alternativas, etc.
Sin lugar a dudas el servicio más importante es el de suministro de electricidad. ¿Es muy común tener micro cortes eléctricos, pero que pasaría si estamos ante una situación de uno o más días sin suministro eléctrico? ¿Qué alternativas tenemos? ¿Compramos un generador? ¿Enviamos a todos los empleados a casa hasta que el servicio sea restablecido? Deberemos también revisar nuestro esquema de telefonía. Ante un desastre de magnitud seguramente lo primero que utilizaremos son los teléfonos, ya sean fijos en algun worksite o celulares. Una vez fijado los sitios alternativos donde los empleados estarán trabajando en caso de desastre, debemos documentar como haremos el ruteo de las llamadas entrantes a estos sitios alternativos o si grabaremos un mensaje grabado indicando a nuestros clientes como contactarnos.

Almacenamiento

Ya vimos anteriormente que no basta con hacer backups todos los días. Ante un desastre debemos de contar con métodos eficientes de recuperación de la información. Es común ver envío de cintas a cajas fuertes en los Bancos, como mitigación del riesgo de no poder disponer de las cintas que tenemos en la empresa (destrucción total del edificio) ¿Pero qué pasa si el siniestro ocurre un viernes a la noche? ¿Esperaremos hasta el lunes a la mañana para poder acceder a las cintas almacenadas en el banco?
Veamos algunos puntos de interés a ser revisados con respecto a almacenamiento:
- ¿Los backups son enviados fuera del edificio de manera regular?
- ¿Cuál es la política de rotación de las cintas o dispositivos de almacenamiento?
- ¿Cada cuánto testeamos las cintas de backups para saber que podés hacer un restore en caso de necesidad?
- ¿Se revisan los logs generados por nuestros sistemas de backups?
- ¿Hay información en laptops o estaciones de trabajo de la cual no estamos haciendo backup y puede ser critica?

Documentación de sistemas informáticos

La documentación de los sistemas informáticos e infraestructura de IT para DRP tiene que estar confeccionada de manera tal que los sistemas críticos puedan ser restablecidos aún por personas no familiarizadas con nuestro trabajo. En el peor de los escenarios, quizás no estemos nosotros ni nuestros equipos para poder restablecer la operatoria.
Es muy común en la cultura latina pensar que

Disaster Reco



"alguien" del departamento de IT estará listo y disponible ante estos casos. No hace falta pensar tan trágicamente, pensemos unos instantes en personas técnicas que son claves en la operatoria de IT cotidiana con mucho conocimiento en las cabezas y no documentado correctamente. ¿Qué pasa si alguna de estas personas repentinamente no esta disponible? Debemos documentar toda la información necesaria para que los sistemas críticos puedan ser restaurados por terceras personas. Por eso es crítico documentar como mínimo lo siguiente:

- Diagrama del Network.
- Credenciales y passwords.
- Direcciones de IP internas.
- Información de cada una de las sucursales o work-sites (dirección, teléfono, tipo de conectividad a la red, inventario de hardware y software, etc.).
- Información de Proveedores y consultores.
- Información de los dominios del network.
- Inventario de software.
- Inventario de contratos.
- Inventario de Hardware.
- Información detallada de sistemas telefónicos y call centers.

Equipos, equipos y más equipos…

Poder administrar, dirigir y controlar una crisis, es sólo posible con el trabajo coordinado de equipos. Vale decir que en estas ocasiones no existe un superhéroe… Aquí SWAT es más importante que Superman.

Veamos una lista de los posibles equipos a ser formados. Ésto depende del tipo y tamaño de empresa para la cual desarrollamos un DRP.

- Aplicativos: restaurar los sistemas informáticos.
- Hardware: restaurar la infraestructura.
- Servicios: restaurar servicios críticos.
- Financiero: asegurar flujo financiero, autorizar gastos.
- Legal: a cargo de todos los temas legales durante la crisis.
- Comunicación: comunicaciones a las diferentes audiencias.
- dirección: panel de control del funcionamiento de todos los equipos.

Tiempos de Caída

Aquí analizaremos junto a las demás áreas de la empresa, las diferentes posibilidades de downtime para cada uno de los escenarios posibles. Algunos de los tópicos a ser considerados son los siguientes:

- ¿Cuál es el peor de los escenarios que tendría nuestra empresa con respecto a downtime y pérdida de información?
- ¿Cuánto es el máximo de tiempo que la empresa puede estar sin servicios claves?
- ¿Cuánto es el costo horario de estar "fuera de servicio"?

Estas preguntas son fundamentales para definir qué tipo de solución de recuperación implementaremos (Mirror Data Centers, Hot Recovery Site, Warm Recovery Site, etc.) y para definir la prioridad en la cual estaremos recuperando los sistemas y servicios ante un determinado escenario.

Empresas con poca tolerancia ante downtimes o pérdidas de información, tendrán que implementar soluciones con redundancia de servicios o Hot / Warm Recovery Sites.

Poder llegar a un acuerdo de cuánto es el costo horario por estar fuera de servicio, nos permitirá entender claramente los costos de downtime en dinero y su impacto financiero en la operatoria de la empresa. Además, sirve para discutir junto con los comités de dirección, las diferentes alternativas de soluciones de DRP contra los costos de estar fuera de servicio. Ésto es una manera de poder llevar a $$$ y hablar en un lenguaje de negocios y no sólo de IT, los conceptos que venimos analizando juntos.

Mantenimiento

Ya sea que hemos decidido por una solución de espejar todos nuestros Data Centers, o si hemos decidido tercerizar este servicio contratando Data Centers a demanda, tenemos que ser muy celosos con el mantenimiento de nuestros planes de DRP. Esto incluye:

- Revisiones del Plan: actualizaciones semestrales o anuales.
- Testeos de la solución: se recomienda hacer un simulacro una vez al año. ■

ZigBee WiMAX Wi-FI

Ezequiel Eduardo Pawelko
Licenciado en Sistemas de Seguridad en Telecomunicaciones
Ingeniero en Telecomunicaciones

WIRELESS PRESENTE Y FUTURO

En este artículo, describiremos las tecnologías inalámbricas que están desplazando a las líneas cableadas, como a su vez los pros y contras de sus respectivos protocolos. Desde tecnologías pioneras a vanguardistas, analizaremos WiFI, WiMAX, y ZigBee.

Las tecnologías inalámbricas (*wireless*) se están imponiendo sobre las tecnologías alámbricas convencionales y diversas son las razones: el alto costo de los cables y de mano de obra, el bajo tiempo de despliegue de los sistemas wireless y la no necesidad de permisos municipales son algunas de las variables que influyen en la decisión a la hora de implementar una red de telecomunicaciones, ya sea como red de acceso (llegada al abonado o usuario final) o de transmisión (enlaces propios de la red de telecomunicaciones).

El tipo de tecnología elegida siempre es función del tipo de servicio a transportar. Hasta hace algunos años era común utilizar wireless en la telefonía rural, donde el costo de despliegue de una red de cobre no se justifica por la densidad de clientes, los sistemas de telefonía celular y los troncales que unen a estos sistemas con las **PSTN** (*Red Telefónica Pública Conmutada*). Hoy día, las tecnologías wireless se usan para la prestación de cualquier tipo de servicio, desde telefonía e **Internet de Banda Ancha** (*Broadband*) hasta, incluso, **Video Bajo Demanda**. Todos los servicios que eran soportados por los medios "alámbricos" (cobre, coaxial o fibra óptica) hoy pueden brindarse a través de sistemas de radio con la misma (o aún mayor) calidad que los sistemas convencionales.

Tal es la aceptación de estos sistemas que se están expandiendo al campo de los sistemas de control, alcanzando todos los lugares donde se requería antiguamente un medio alámbrico que soporte la información.

El camino de desarrollo masivo, se inició en el mundo de las LAN's con **WiFI** (*Wireless Fidelity*) y cuyo Estándar Internacional es el 802.11 del IEEE (Instituto de Ingenieros Eléctricos y Electrónicos). Dicho estándar jugó un papel fundamental en el desarrollo de estos sistemas, ya que demostró un cambio de paradigma de lo alámbrico a lo inalámbrico.

El desarrollo de **WiFI** llevó a **WiMAX** (*Worldwide Interoperability for Microwave Access*), cuya tecnología es más sofisticada y su función es complementar a WiFI para poder cubrir áreas más amplias.

El último paso en las comunicaciones wireless lo constituyen los sistemas **ZigBee**, cuya aplicación se orienta al campo de los sistemas de control.

Desarrollo de WiFI

WiFI es una alianza de empresas que lleva adelante el **IEEE 802.11** y se ha transformado en el nombre de mercado del estándar 802.11. Dicho estándar permite hacer LAN's inalámbricas en una de dos configuraciones: con una estación base, denominada Access Point, o sin dicha estación, denominada red Ad Hoc.

El 802.11 ha pasado por diferentes revisiones que han dado como fruto distintas versiones, las cuales emplean diferentes técnicas de modulación y soportan diferentes velocidades de transmisión de información.

Como se ha comentado, WiFI se diseñó para crear LAN's inalámbricas, por lo que su alcance es pequeño en relación a otras tecnologías como WiMAX que se orientan a conexiones de area amplia. WiFI debe comprenderse como una extensión de LAN Ethernet o como una LAN en sí que posee todos los mecanismos necesarios para que sobre ella pueda correr la suite TCP/IP u otra suite.

El estándar 802.11 de ´97 especificaba tres técnicas de transmisión para la capa física, diferenciadas por su tecnología de modulación.

La primera de las técnicas fue la de **transmisión infrarroja**, la cual es de bajo costo pero de corto alcance.

El segundo estándar de '97 corresponde al **FHSS 802.11** (*Frecuency Hopping Spread Spectrum*). Esta tecnología es sumamente interesante por su alta seguridad y alta inmunidad al ruido. La seguridad del FHSS nace de su principio de funcionamiento y no de algoritmos de cifrados, ni algo por el estilo. Cuando dos terminales FHSS 802.11 quieren transferirse información, lo hacen transmitiendo la misma en diferentes frecuencias, pero sólo en una frecuencia a la vez. La elección de la frecuencia a transmitir en un momento dado es determinada antes de comenzar la transmisión y la seguridad del sistema radica en lo aleatorio o impredecible que sea la secuencia de saltos a elegir.

Su alta inmunidad al ruido reside en que se transmite en una pequeña y distinta porción del espectro en cada momento, por lo que el ruido que afecta a una parte de ese espectro sólo afectará la transmisión cuando se esté transmitiendo en esa parte del mismo.

El 802.11 utiliza en todas sus versiones dos bandas de frecuencias del espectro radioeléctrico denominadas **ISM** (*Bandas Industriales, Médicas y*

Científicas, que corresponden a las frecuencias de **2,4 GHz** y **5,8GHz**), las cuales son bandas de frecuencias en las que se puede transmitir prescindiendo de una licencia que reglamente su uso. Es común llamarlas "bandas no licenciadas", y la FHSS es una de las pocas técnicas recomendadas por la **FCC** (organismo estadounidense encargado de regular las telecomunicaciones en dicho país, pero de gran influencia en el contexto mundial) para utilizar en estas bandas.

Como las bandas ISM no requieren licencia, nada impide que en un momento dado se encuentren en funcionamiento varios sistemas FHSS al mismo tiempo, lo cual haría que las frecuencias de las tablas de Hop's (secuencia de frecuencias a saltar) se superpongan. El hecho de que dos equipos transmitan al mismo momento y en la misma frecuencia hace que las tramas de información transmitidas en ese período se pierdan. Sin embargo, la conectividad no se perderá, ya que las tramas serán retransmitidas, en el próximo salto de frecuencia, debido a que las secuencias de saltos de ambas comunicaciones serán distintas.

El tercer estándar del IEEE 802.11 del '97 es el **DSSS 802.11** (*Direct Secuence Spread Spectrum*). DSSS es una técnica de Capa Física que tiene la característica de presentar alta seguridad, confiabilidad y eficiencia espectral. DSSS (a diferencia de FHSS, el cual transmite en porciones pequeñas de la banda ISM) utiliza toda la banda de frecuencia ISM, aún ante la presencia de ruido, y emplea técnicas matemáticas avanzadas para poder distinguir la señal de información en un espectro amplio y sumamente polucionado de interferencia.

La seguridad que presenta DSSS es muy alta y radica en la utilización de un código binario que funciona como una especie de "llave criptográfica para codificar y decodificar la información".

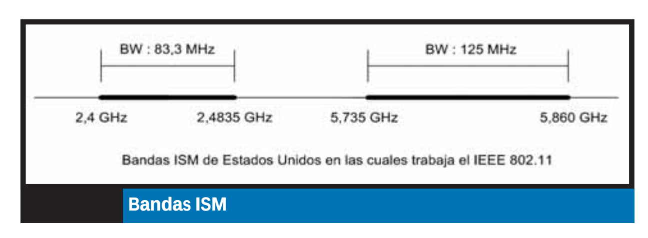
La FCC, exigía hasta el 2002 que todas las comunicaciones que se realizaran en las bandas ISM se hicieran en el modo **Spread Spectrum** (*FHSS* o *DSSS*). Levantado dicho requisito, como consecuencia de la aparición de tecnologías más eficientes, se creó el **IEEE 802.11a**, el cual utiliza una tecnología llamada **OFDM** (*Multiplexación por División de Frecuencias Ortogonales*).

El IEEE 802.11a permite transmisiones de hasta **54 Mbps** en la banda ISM más ancha, de **5 GHz**.

El OFDM empleado en IEEE 802.11a es una tecnología que emplea modulación en multiportadoras, 52 portadoras en total, con un mecanismo análogo al del ADSL, sólo con la salvedad de que el 802.11a es inalámbrico.

OFDM, al igual que FHSS y DSSS, es considerada una técnica de Spread Spectrum por transmitir en un amplio rango de frecuencias al mismo tiempo. La ventaja de OFDM respecto a las otras técnicas es que es libre de ruido debido a que las portadoras son afectadas por el éste de distinta manera), y tiene una alta eficiencia espectral, ya que utiliza modulación N-QAM, la cual permite transmitir muchos bit por Hertz o baudio.

Al IEEE 802.11a le siguió el **IEEE 802.11b**, el cual utiliza **HR-DSSS** (*Espectro Disperso de Secuencia Directa de Alta Velocidad*) y que no es más que un DSSS de alta capacidad, y el **802.11g**, que emplea OFDM en la banda ISM de *2,4 GHz*, entre otros estándares del 802.11 menos significativos.



Bandas ISM

Es innegable el éxito del estándar 802.11 en cuanto a su crecimiento exponencial y al romper con el paradigma del cable en las redes de datos Ethernet. También se hace evidente el éxito de la tecnología al comenzar a aplicarse en redes que exceden las aplicaciones Wireless LAN. El 802.11 no tiene un competidor robusto que lo remplace, y es probable que los chips que lo integran también soporten otras tecnologías como WiMAX.

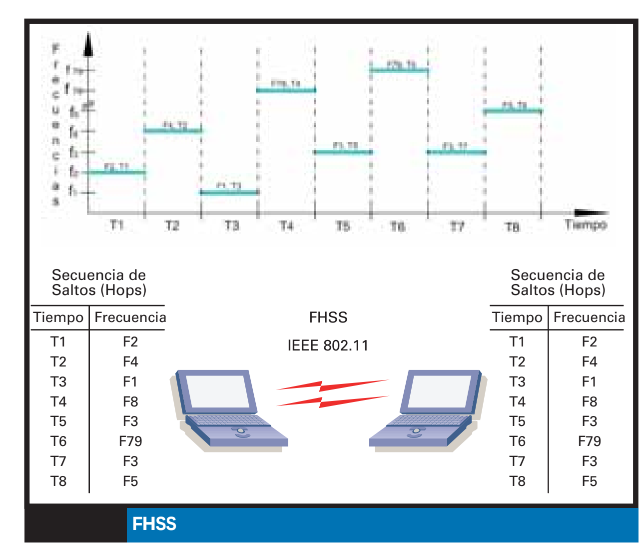
Banda Ancha Inalámbrica en Redes de Área Metropolitana

El IEEE 802.11 es una solución de conectividad inalámbrica en redes LAN, de manera que puede extenderse el alcance de las redes Ethernet. Tal fue el grado de aceptación de esta tecnología (siendo principales determinantes el bajo costo y la facilidad de implementación) que muchos pequeños proveedores de servicios de telecomunicaciones se vieron tentados a utilizarla para transportar sus servicios en despliegues del tipo **MAN** (*Red de Área Metropolitana*). Dichos proveedores transportan Internet de Banda Ancha e incluso y Telefonía IP. Si bien es común encontrar estos despliegues, la tecnología 802.11 o WiFI no es realmente apta para tal hazaña en la mayoría de los casos.

El IEEE 802.11 tiene serias limitaciones en la prestación de servicios de telecomunicaciones en zonas amplias. Las razones son varias y determinantes. El 802.11, como se ha comentado, trabaja en bandas de frecuencias "*no licenciadas*", las bandas ISM. El término "*no licenciado*" no quiere decir que no se requiera registrar el enlace, ya que la **CNC** (*Comisión Nacional de Comunicaciones*) exige tal acto, sino de que no se requiere tramite de licenciamiento. Las ventajas de costo y licencia que poseen las aplicaciones Wireless LAN no se materializan en las aplicaciones **Wireless MAN** (*Red de Área Metropolitana Inalámbrica*). La realidad demuestra que las bandas ISM se encuentran ampliamente polucionadas de radiación interferente proveniente de todos los sistemas irradiantes que trabajan a tales frecuencias, además del ruido industrial. Recordemos que los hornos de microondas, los teléfonos inalámbricos hogareños, los controles remotos de los portones de garajes y toda una serie de sistemas de baja potencia trabajan en dichas frecuencias, y que cada uno de ellos es un potencial interferente para todos los demás. La conclusión al respecto es que no es posible dar un servicio con calidad si se transmite en una zona espectral ampliamente polucionada. El servicio de Internet, cuando se utiliza para navegar en la Web, no es tan sensible a las variaciones en la calidad de los enlaces, pero sí lo son los servicios interactivos o en *Real Time*. Los servicios de voz o video conferencias, como la *Telefonía IP* o el *H.323*, respectivamente, demandan muy alta calidad en la conexión. La pérdida incesante de datagramas como consecuencia de la interferencia, disminuye notablemente la calidad de las comunicaciones. Una consideración a nivel de las Capas superiores del Modelo OSI es que la suite TCP/IP no ha sido diseñada para trabajar en redes inalámbricas y su empleo es de compromiso.

La solución al problema anterior es utilizar una banda de frecuencia libre de interferencia, es decir, una banda licenciada. Estas bandas son utilizadas sólo por el titular actual de la licencia, por lo que desaparecen los problemas antes mencionados. Los inconvenientes que ahora se presentan son el costo, la disponibilidad de licencias y el hecho fundamental de que los equipos IEEE 802.11 o WiFI sólo trabajan en bandas "no licenciadas", por lo que se puede descartar esta solución. Muchos proveedores de servicios de telecomunicaciones, al alcanzar un tamaño considerable, adquirieron soluciones Wireless propietarias y licencia de espectro para ser consistentes con los servicios soportados.

La segunda y gran limitación que posee WiFI para ser utilizada en soluciones Wireless MAN es que no posee mecanismos reales que garanticen **Calidad de Servicio** o **QoS** (*Quality of Service*), los cuales son requisito en las redes que presten ser-



Tiempo	Frecuencia
T1	F2
T2	F4
T3	F1
T4	F8
T5	F3
T6	F79
T7	F3
T8	F5

Tiempo	Frecuencia
T1	F2
T2	F4
T3	F1
T4	F8
T5	F3
T6	F79
T7	F3
T8	F5

FHSS

vicios sensibles al *Delay* (demora) y/o *Jitter* (variación de la demora de los paquetes). La QoS fue algo que se les escapó a los diseñadores de redes LAN por muchos años. La QoS nace en las redes **WAN** (*Redes de Área Amplia*) y se generalizó a todas las tecnologías que transportan tráfico sensible. Las redes Ethernet, para alcanzar este requisito y ser capaces de transportar multiservicios (servicios *H.323* o *SIP*), emplean actualmente mecanismos similares llamados **CoS** (*Class of Service*). Los mecanismos reales QoS permiten dar prioridad al tráfico sensible de manera que éste sea el primero en fluir (esperar 500 mseg más un datagrama que transporta un segmento de página Web no es tan crítico como el hecho que un datagrama que transporta voz tenga 500 mseg de Jitter, siendo que a los 150 mseg el oído es sensible). Para solucionar este problema los diseñadores de AP utilizan mecanismos de control de calidad de servicio, pero a nivel de **Capa 3** (*Network*), como **ToS** (*Type of Service*) o **Diff Serv.** (*DSCP, Servicio Diferencial*) y actualmente a nivel de Capa 2 con el **IEEE 802.11e** que poco hace respecto de la QoS. El IEEE 802.11e fue un intento del IEEE para ser consistente con las aplicaciones multimedia (SIP y H.323) pero es un sistema de "*mejor esfuerzo*" en lugar de ser un sistema real que procure garantizar la priorización del tráfico sensible. La razón anterior, surge de que los terminales IEEE 802.11 son los que configuran la QoS que desean, por lo que ellos podrían configurar la prioridad de un e-mail al mismo nivel que el tráfico de voz, y el Access Point así lo considerará. Tal es el fracaso técnico de IEEE 802.11e, en entornos exigentes, que los diseñadores de AP utilizan sistemas de QoS paralelos, como los ya nombrados, y que no pertenecen al estándar.

Otra limitación del protocolo es la relativamente **baja confiabilidad** de los equipos por cuestiones de costos. Los equipos WiFI tienden a ser de bajo precio y los AP se diseñan para capacidades de usuarios concurrentes generalmente inconsistentes con el hardware que los procesa.

La **potencia** es otro requisito. La FCC restringe la potencia en las bandas ISM, por lo que los equipos transmiten con baja potencia. Para poder alcanzar distancias mayores se requiere emplear antenas parabólicas de alta ganancia y por lo tanto de alto costo, quedando la calidad del enlacé librada a la suerte.

La última incapacidad del IEEE 802.11 en aplicaciones metropolitanas es la necesidad de tener línea de vista o **LoS** (*Line of Sight*, que hace referencia a la visión entre antenas), lo cual no es posible en las zonas de topología compleja, como por ejemplo en las ciudades donde hay edificios que obstaculizan la visión.

Por las razones nombradas se hace evidente que WiFI ó IEEE 802.11, siendo diseñado exclusivamente para Wireless LAN, no es una solución para la mayoría de las veces donde se deba realizar una red inalámbrica de área metropolitana, por lo que el IEEE desarrolló el 802.16.

WiMax

WiMax es una alianza de empresas que impulsan el desarrollo del estándar 802.16 del IEEE. WiMax fue diseñada desde sus comienzos para cubrir zonas metropolitanas, por lo que es una tecnología de Wireless MAN. El estándar no se diseñó para reemplazar al 802.11, Wireless LAN, sino que satisface una necesidad diferente. **Los estándares 802.11 y 802.16 se complementan**: el primero satisface la conectividad inalámbrica **LAN**, y el segundo, la conectividad inalámbrica **MAN**.

El 802.16 nace como una alternativa a las redes de acceso telefónico cableadas. Todo surgió con la desregulación del sistema telefónico a nivel mundial. Desde el momento en que se permitió que nuevas empresas de telecomunicaciones prestaran servicios de telecomunicaciones en las zonas de las grandes empresas monopólicas, se supo que la única manera de hacerlo era de forma inalámbrica debido al excesivo costo de instalación de cables de cobre, fibra óptica, coaxial, par trenzado o cualquier otro medio que requiera obras civiles para su instalación. La solución sin duda eran las ondas radioeléctricas, por lo que las empresas competidoras se introdujeron en el mercado colocando grandes antenas, tipo celular, para cubrir zonas amplias. La primera tecnología usada se denominó **LMDS** (*Servicio Local de Distribución Multipunto*), la cual es una tecnología de *multimegabit* que permite el transporte de voz paquetizada, Internet de Banda Ancha e incluso Video Bajo Demanda. El problema de LMDS era que no existía un estándar aceptado de manera que los precios sean bajos como consecuencia de la aceptación y producción a gran escala. Por estas razones, el IEEE en 1999 creó un grupo de trabajo para lograr un estándar de **Broadband Wireless** (*Banda Ancha Inalámbrica*) el cual se aprobó en el 2002 comenzando con la evolución 802.16, hoy conocido por WiMax.

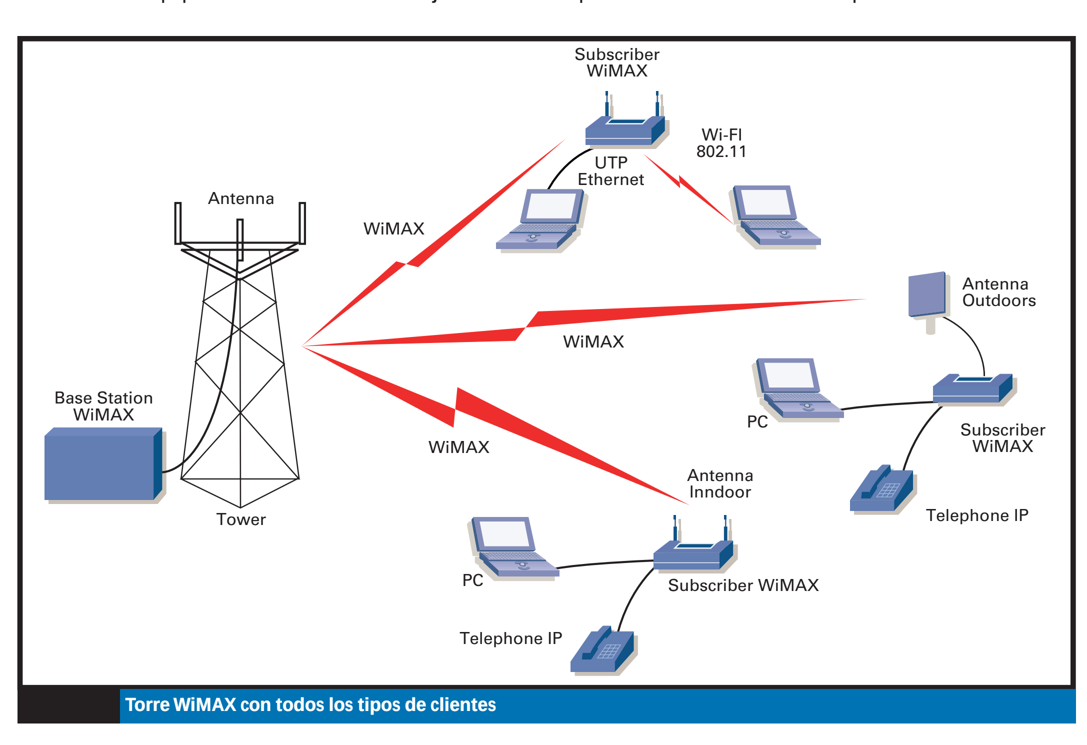
Características de WiMax

WiMax es una tecnología que se desempeña plenamente con cualquier tecnología de Capa 3. Se denomina a menudo como elemento de las llamadas **NGN** (*Redes de Siguiente Generación*).

WiMax es una solución de acceso, lo que significa que forma una topología punto-multipunto con un concentrador en el centro, denominado **Base Station**, y los terminales en los bordes, denominados **Subscribers**, que permiten transportar los servicios de telecomunicaciones hasta la sitio del abonado o usuario.

A diferencia de WiFI, que se la utiliza en distancias de, como máximo, algunos cientos de metros, WiMax alcanza distancias de hasta 50 km. La causa de estas magnitudes está muy relacionada con el hecho de que esta tecnología trabaja en bandas licenciadas, aunque también lo hace en bandas no licenciadas. La razón de hacer que trabaje en bandas sin licencias es que se podría utilizar para propósitos de rápido despliegue, (militar o catástrofes), o en aplicaciones que no justifiquen obtener una licencia y para continuar con el espíritu de "banda libre" que impulso a WiFI.

WiMAX permite transportar información hasta los *75* Mbps, que es más de lo que permiten transportar cualquiera de las tecnologías alámbricas como *XDSL* o *Cable Módem* e incluso *Acceso por Fibra*. WiMAX no requiere *Línea de Vista*, es decir que trabaja en modo NLOS, pues utiliza OFDM a nivel físico obteniendo así altas velocida-



Torre WiMAX con todos los tipos de clientes



des de transmisión de datos y alta eficiencia espectral. La disposición de las antenas es en celdas, como lo hacen los celulares, ya que se espera que la próxima generación WiMAX soporte movilidad (capacidad de poder pasar de una celda a otra sin perder comunicación, como lo hacen los celulares) de manera que los usuarios puedan ser móviles.

La última de las características que se torna en una ventaja competitiva es que WiMAX soporta Quality of Service. El IEEE 802.16 definió cuatro tipos de calidad de servicios: **Tasa de bit constante** (se utiliza para el transporte de circuitos sincrónicos, como *E1* ó *T1*), **Tasa de bit variable en tiempo real** (se emplea para la transmisión de multimedia comprimida, como *H323*), **Tasa de bit variable no en tiempo real** (se usa en la transmisión de archivos o datos) y **Servicio por el mejor esfuerzo** (este servicio corresponde a la capacidad de procesamiento y transporte residual del sistema).

Conclusión acerca de WiMax

WiMAX no es sólo el **futuro**, es **presente**, y en la Argentina son varias las empresas de telecomunicaciones que están empezando a dar servicios con esta tecnología y son diversas las que están proyectando sus redes de este modo. Las pruebas de campo han demostrado que las velocidades e incluso la calidad de las transmisiones han superado las expectativas y que ésto ha hecho que se afiance como una verdadera **NGN** (*Red de Siguiente Generación*). También es cierto que el 802.16 todavía no dio lo mejor de sí y que ésto va a ocurrir cuando el estándar contemple la movilidad de usuarios, la cual se verá en muy poco tiempo.

ZigBee

ZigBee es un protocolo de comunicaciones inalámbricas basado en el estándar **IEEE 802.15.4** del 2003 y cuya función es solucionar los problemas de interoperabilidad, duración de la batería y costos de los protocolos propietarios en las aplicaciones de **domótica** (*home automation*).

Al igual que WiFI y WiMAX, ZigBee posee una alianza de empresas, **ZigBee Alliance**, y cuyo objetivo es desarrollar software de comunicaciones basado en el IEEE 802.15.4 e incentivar su desarrollo. La filosofía de aplicación es distinta a la del IEEE 802.11 y del IEEE 802.16 ya que este estándar se utiliza principalmente para aplicaciones domóticas donde la capacidad de transferencia de información requerida es mínima y el costo y el consumo juegan un papel fundamental. El protocolo se utiliza para controlar la iluminación, calefacción, el sistema de seguridad, etc. de cualquier casa o edificio de los llamados inteligentes. Se espera que ZigBee se aplique a componentes electrónicos, sistemas de control automático, aplicaciones industriales, periféricos de PC, aplicaciones médicas, juguetes y juegos siendo actualmente la aplicación principal los sistemas de demóticas y de automatización.

ZigBee posee una arquitectura basada en el modelo **OSI**. El IEEE 802.15.4 define las dos capas más bajas: **La Capa Física** y la **Subcapa de Control de Acceso al Medio** de la **Capa de Enlace de Datos**, la cual se encarga de aislar los detalles de las tecnologías físicas a la capa de Control de Acceso al Medio. Dichas capas son utilizadas por ZigBee para crear un marco de trabajo para las aplicaciones.

La Capa Física del IEEE 802.15.4 puede trabajar en uno de tres rangos de frecuencias: **868 MHz**, **915 MHz** o **2.4 GHz** con velocidades de hasta **20 kbps**, **40 kbps** y **250 kbps** y cuya utilización de bandas de frecuencias es **Europa**, **Estados Unidos** y el **resto del mundo**, respectivamente. La norma IEEE 802.15.4 permite alcanzar distancias de hasta **100 metros** con muy baja energía, lo que la hace práctica en la mayoría de aplicaciones domóticas.

La energía siempre fue un problema en todas las aplicaciones de control. Los productos Zigbee pueden funcionar con tan bajo consumo de energía que las baterías pueden durar años, más de mil veces que en otros sistemas de comunicaciones inalámbricas.

La tecnología ZigBee soporta tres tipos de topologías de red para que se comuniquen los dispositivos. La primera de ella es la topología Star, o *Estrella*, la cual presenta larga vida útil como consecuencia del bajo consumo de energía requerido. La segunda es la topología **Mesh**, o *Malla*, en la cual existen múltiples rutas para alcanzar un destino obteniéndose alta confiabilidad. La tercera y última de las topologías es la **Cluster Tree** (*racimo de árbol*) la cual es una topología del tipo **Mesh-Star** que encierra los beneficios de ambas.

La razón por la cual se espera que ZigBee sea un éxito en este campo, como lo es WiFI en el Wireless LAN, se debe a su reducido costo, fácil despliegue, interoperabilidad, alta velocidad (para este tipo de aplicación), bajo costo de instalación, confiabilidad, escalabilidad, multi-topología y a que no hay límites para con las aplicaciones.

Conclusión

Las tecnologías inalámbricas actuales son el inicio de una era inalámbrica. Esta nueva era se destaca por el reemplazo de cable por ondas Hertzianas que colapsarán el Espectro Radioeléctrico de los países. WiFI ya hizo lo suyo respecto del espectro en la mayoría de los lugares de alta densidad poblacional saturando las bandas ISM. ZigBee competirá con WiFI en la banda de 2,4 GHz y con otras aplicaciones de telecomunicaciones en las bandas ISM más bajas. WiMAX, según se espera, trabajará principalmente en bandas licenciadas, por lo que se presentará una sobredemanda de las frecuencias más favorables a la propagación electromagnética, como la banda de **3,5 GHz**, por parte de los portadores. El desafío está presente en los organismos nacionales que regulan el Espectro Radioeléctrico de cada país ya que éstos deberán procurar tomar las decisiones que más favorezcan a los usuarios, administrando eficientemente el Espectro.

Hoy tenemos posibilidades de transmitir cualquier tipo de servicio o información, sin importar sus exigencias técnicas, de manera inalámbrica al abonado, usuarios o aplicación de control. En el acceso a los usuarios, antes transportábamos telefonía en un enlace de baja capacidad y calidad y hoy acercamos Telefonía IP, acceso a Internet de Banda Ancha e incluso se está empezando a brindar servicios de Video Bajo Demanda con la más alta calidad, obteniéndose el transporte de todos los servicios de telecomunicaciones existentes. **Los costos de las redes de telecomunicaciones disminuyeron en factores de más de 10**, gracias a tecnologías como WiMAX y la posibilidad de llegar a zonas de menor densidad poblacional pudiendo acercar servicios que hoy se consideran casi *Servicios Básicos* por su necesidad, como Internet.

ZigBee, WiFI y WiMAX tienen mucho más para dar y eso se verá con la madurez de estos sistemas y la disminución en los costos. ■

¿Moda o innovación estratégica?

Repaso de la historia e histeria de la VIRTUALIZACIÓN

Maximiliano S. Di Toro
Network Administrator

La idea de máquina virtual nace con la salida del sistema VM/370 de IBM a principios de los '70. Su objetivo era dar la posibilidad de correr varios sistemas operativos a la vez, en la misma computadora. Para ésto, no solo emulaba en paralelo el sistema operativo y el hardware, sino que hacía de nexo coordinante entre ambos.

El corazón del emulador era conocido como monitor de máquina virtual, y se ejecutaba sobre el hardware, ésto le proporcionaba varias máquinas virtuales a los sucesivos sistemas operativos emulados. Estas máquinas virtuales eran copias exactas del hardware.

Por ésto, cada una podía estar ejecutando cualquier sistema operativo.

Buscando darles a los usuarios de Macintosh la facilidad de correr aplicaciones en un entorno Windows sobre procesadores Intel (combinación conocida popularmente como Wintel) Insignia Solutions fue el pionero en la virtualización creando "**Softwindows**", mientras que aparecían productos similares como **Virtual PC** de Connectix.

La posibilidad de ejecutar aplicaciones Intel sobre el Macintosh era sólo parte de la solución. Probablemente el usuario deseaba también intercambiar datos entre ambos entornos, en ocasiones alguna línea de texto, en otras documentos de gran tamaño, para ello cada una de las plataformas disponía de un grupo de herramientas orientadas a ese fin. Ambos entornos daban la posibilidad de definir carpetas del Macintosh como discos del PC.

Virtual PC permitía realizar este proceso con un gran número de carpetas, para ser exactos hasta que se acabasen las letras de asignación, ya que cada carpeta recibía una letra de disco:"**F:** ", "**G:** ", etc. siendo posible que estas asignaciones fueran permanentes o sólo vigente durante la sesión actual. SoftWindows tenía definido inicialmente este valor de carpetas compartidas en tres, pero podía ampliarse modificando un archivo del sistema de Windows.

VMWare (www.vmware.com) era otro de los productos virtualizadores, teniendo diferencias en la arquitectura para afectar la forma en la que el software interactúa con el equipo (hardware). Dependiendo del propio ordenador donde funcione, el rendimiento del sistema virtual o emulado puede variar. Connectix lanzo Virtual PC a un precio más reducido, Insignia entró en crisis y terminó vendiendo Softwindows a FWB Software, saliendo así del mercado.

En junio de 1998 Apple España lanza una campaña dirigida al mercado educativo por la que, al adquirir un ordenador Power Macintosh G3, el cliente recibe como obsequio 32 MB

Virtual PC de Connectix.

En sus comienzos adoptando una estrategia más radical trataba de virtualizar directamente la totalidad del hardware de un ordenador PC . Para ser exactos, y según se indicaba en el manual, implementaba un procesador Pentium MMX con MMU, FPU y modo protegido, una placa con arquitectura Triton de Intel (una de las arquitecturas de chips más extendidas de la industria de es entonces), MR BIOS, controladora IDE/ATAPI de disco duro y CD-ROM, tarjeta de vídeo S3 928 con capacidad de hasta 2 Megabytes de VRAM, dos puertos serie estándar de PC, tarjeta de sonido SoundBlaster Pro y tarjeta Ethernet DEC 21041.

soluciones inteligentes
poweredbycisco.

Implemente la Solución de Comunicaciones IP de Cisco
y sume un activo estratégico a su empresa.
Incorpore nuevas aplicaciones que le permitirán ahorrar costos,
incrementar su productividad y aumentar la satisfacción de sus clientes.
Sólo quien más sabe de redes puede brindarle la solución de comunicaciones
más segura que integre voz, video y datos en una única red.
Descubra la experiencia, tecnología y soporte de Cisco
en **www.cisco.com/offer/nexitipc**
o comuníquese al **0810-444-CISCO (24726).**



customer satisfaction. powered by

SoftWindows 95.

Su funcionamiento se basaba en virtualizar un procesador Intel con Windows 95 instalado (una versión anterior incorporaba Windows 3.1). Para ello los desarrolladores crearon el virtualizador del procesador y además modificaron los archivos del sistema de Windows de forma que las llamadas realizadas al sistema operativo, por parte de las aplicaciones, para acceder al hardware: video, disco duro, disquetera, etc. se convierten directamente en código Macintosh.

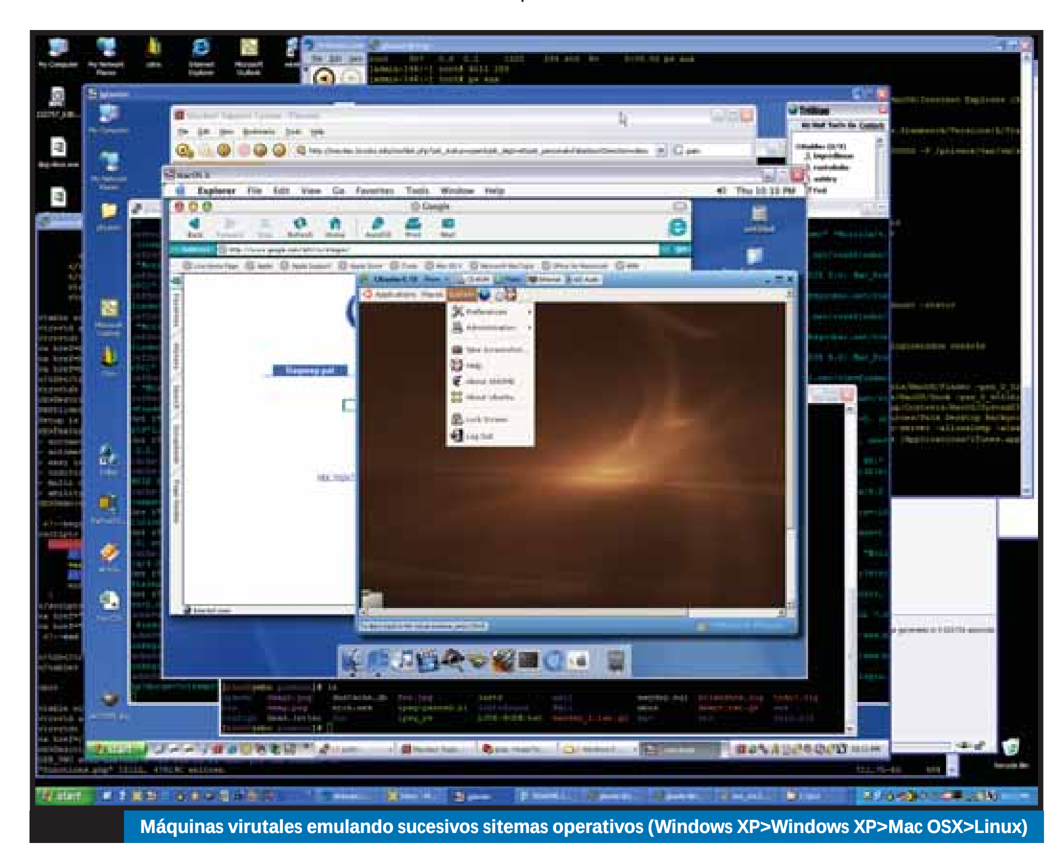
de memoria RAM adicionales y el software Virtual PC 2.0 DOS de la firma Connectix Corp. para compatibilidad con el entorno PC.
El nuevo producto de Connectix incorporaba la posibilidad de correr cualquiera de las versiones Windows de aquel momento e incluso ejecutar aplicaciones escritas para D.O.S. y OS/2, de IBM y después, aunque parezca contradictorio, sacó la versión para Windows, virtualizando así un entorno Macintosh pero sin hacer modificables algunas configuraciones, lo cual no lograba sacar provecho de toda la capacidad del hardware ni del sistema Mac OS.
En el año 2003 Microsoft adquiere a Connectix. La razón, al parecer, puede estar dada en que Microsoft quiso asegurar la transición entre Windows NT4 y Windows Server 2003 y defender así la implantación de Windows en los servidores.
Por un lado, Microsoft temía a las alternativas Linux/Unix apoyadas especialmente por IBM, HP y Sun. Por el otro, lograba tener un "as" bajo la manga si Apple decidía atacar en su terreno a Microsoft.
Al saber que Microsoft compró a Connectix, FWB Software retomó el desarrollo de Real PC y Softwindows, y a mediados del 2003 saco su beta, a pesar de que Microsoft le había iniciado juicio.
Microsoft sacó entonces su primer Virtual PC con la tecnología de Connectix, bien, pero ¿Qué era este producto?

Microsoft Virtual PC 2004.

Gracias a Virtual PC los usuarios pueden ejecutar dos o más sistemas operativos de manera simultánea en sus equipos.
Una vez que Virtual PC está instalado en un sistema, puede crear una o más máquinas virtuales. Se puede instalar y configurar un sistema operativo invitado sobre la máquina virtual y entonces, se pueden instalar aplicaciones sobre el sistema operativo invitado. Se pueden crear varias máquinas virtuales, tantas como la memoria permitan y ejecutarlas al mismo tiempo en el mismo equipo. Un cliente puede colocar una de las máquinas virtuales en primer término con tan solo hacer clic sobre la barra del título.
Cada una emula un equipo independiente con su propio sonido, video, adaptadores de red, su propio procesador y existe en un entorno independiente y aislado o bien conectado vía ethernet.
Los cambios que se realizan dentro de las mismas no afecta al ordenador físico en el que se encuentra.
Los usuarios pueden ejecutar varios sistemas operativos de manera simultánea y cambiar de uno a otro sin necesidad de tener que reiniciar el equipo.
Virtual PC imita a los ordenadores reales con tal fidelidad que las aplicaciones instaladas por los usuarios son incapaces de distinguir entre la máquina virtual y la real. Además de este producto para "clientes", lanzó Microsoft Virtual Server 2005 (luego 2005R para 64 bits)

¿Y ahora qué?

Las utilidades que se les puede dar no sólo terminan en poder jugar al mismo tiempo 3D Pinball de Windows en la Virtual PC y en la **PC Física**, sino que los desarrolladores de programas pueden probar en una maquina virtual en tiempo real el software sin poner en riesgo su PC, como así también hacer tests de seguridad creando una red entre la maquina virtual y nuestra computadora. Piensen que también podemos estar corriendo diferentes servicios en cada una de las maquinas virtuales, pero de todas formas si queda vulnerado el sistema huésped todo será en vano.
Otra será la historia con la tecnología Hipervisor. El hipervisor es el kernel simplificado de un sistema operativo que corre directamente sobre el hardware, resultando en un diseño más eficiente que acepta las llamadas al sistema operativo para ciclos del procesador, datos de la memoria y servicios de redes en vez de interceptarlas. Divide los recursos disponibles entre máquinas virtuales basados en porcentajes establecidos por un administrador y reduce el acierto en desempeño del CPU a 5% o menos.
Hace ya más de un año, VMware introdujo su tecnología de Hipervisor x86, el ESX Server, mientras que Microsoft, con ayuda de sus activos Connectix, construyó un hipervisor en la versión Longhorn del Windows Server. Con ésto, aceptará cualquier otro sistema operativo x86, junto con Windows, volviendo mucho más fácil que Windows y Linux corran en la misma máquina.
Xen es el hipervisor open source desarrollado por la Universidad de Cambridge que ha conseguido el apoyo de los fabricantes para convertir la virtualización en una herramienta de infraestructura básica en los centros de datos. El software se popularizó entre casas de bolsa de Wall Street que el año pasado solicitaron a sus autores de Cambridge que formaran una compañía, XenSource, para darles soporte.
La segunda versión de Xen está respaldada por HP, IBM, Sun Microsystems y otras compañías interesadas en estandarizar la virtualización, de manera que puedan disponer de los productos para que trabajen con él.
Cualquier distribución de Linux (RedHat, SuSE, Debian, Mandrake) puede funcionar sin modificar el OS. Además de Linux, los miembros de la comunidad de usuarios de Xen han contribuido o están trabajando para aceptar a otros sistemas operativos tales como NetBSD (Christian Limpach), FreeBSD (Kip Macy) y Plan 9 (Ron Minnich). Una versión anterior de Xen fue desarrollada para Windows XP, pero no estará disponible, para el lanzamiento de su nueva versión, debido a las restricciones de la licencia.



Máquinas virutales emulando sucesivos sitemas operativos (Windows XP>Windows XP>Mac OSX>Linux)

100% FLEXIBLE
100% INTEGRADO
100% CONFIABLE





Microsoft® SQL Server® 2005

100% LISTO
0% ESTRES

Los servidores basados en procesadores Intel® y Microsoft SQL Server® 2005 brindan una solución de base de datos que ofrece importantes mejoras de escalabilidad, entorno de desarrollo, seguridad y confiabilidad para las aplicaciones más exigentes.
Esta combinación le otorga el nivel de performance necesario para llevar adelante su empresa y prepararla para los desafíos de negocio que presenta el futuro.

intel®

Microsoft®

Para más información visite www.intel.com/performance

buscando que hacer éste verano?

Cursos de **Verano** en Central**TECH**

ÚLTIMAS VACANTES INSCRIBITE YA!

MCSE
Capacitate y obtené la certificacion técnica de mayor prestigio del sector.

Lx Expert
En CentralTECH podrás obtener la Capacitación requerida para convertirte en un experto de Linux.

WD Expert
Conocé a fondo los secretos del diseño de páginas web, sus ventajas y sus herramientas.

MCP
Curso intensivo de 40 hs. de duración, orientado exclusivamente a obtener la certificación MCP.

SQL
Para desempeñar exitosamente la función de administrador de bases de datos SQL de Microsoft.







Av. Corrientes 531 - Primer Piso - C1043AAF - Capital Federal - Tel./Fax.: (011) 5031-2233 -
masinfo@centraltech.com.ar
www.centraltech.com.ar



Carreras y Certificaciones en CentralTECH:

Las carreras y certificaciones dictadas en **CentralTECH** aportan los conocimientos y la competencia de los profesionales en el manejo de productos IT. Si representa a un negocio que busca líderes en tecnología o es un profesional de la tecnología de la información, encontrará dentro de nuestro Plan de Carreras la capacitación en las últimas tecnologías.

Plan de Carreras CentralTECH:



CISSP (Certified Information Systems Security Professional) diseñada para capacitar a los profesionales de IT de su empresa con el alto grado de profesionalismo necesario en el area de Seguridad Informática.



MCP (Microsoft Certified Professional) es la certificación básica para los profesionales Microsoft. Ud. puede ser Microsoft Certified Professional y elegir su orientación, rindiendo satisfactoriamente un sólo examen.



MCSA (Microsoft Certified Systems Administrator) es la certificación para administradores de redes y entornos de sistemas basados en plataformas Microsoft Windows. Las especializaciones incluyen MCSA Messaging y MCSA Security.



MCSE (Microsoft Certified Systems Engineer) es la certificación para aquellos profesionales que diseñan e implementan soluciones de infraestructura basadas en plataformas Windows y software de servidores Microsoft. Especialización en Messaging y/o Security.



MCAD (Microsoft Certified Application Developer) está orientada a profesionales que utilizan tecnologías Microsoft para desarrollar y mantener aplicaciones de alto nivel, componentes, clientes WEB o de escritorio y servicios de datos back-end.



MCSD (Microsoft Certified Solution Developer) es la certificación idónea para profesionales que diseñan y desarrollan las últimas soluciones empresariales con herramientas de desarrollo, tecnologías y plataformas de Microsoft y con arquitectura Microsoft Windows.



MCDBA (Microsoft Certified Database Administrator) es la certificación premier para profesionales que implementan y administran bases de datos en Microsoft SQL Server 2000 sobre plataformas Microsoft Windows Server 2003.



MCT (Microsoft Certified Trainer) lo certifica como experto en formación de tecnologías, productos y soluciones Microsoft. Los Partners de Learning Solutions utilizan MCTs a la hora de ofrecer formación en Carreras Microsoft.



LINUX COMPLETA Orientada para aquellos que estén interesados en incursionar en los conceptos básicos del sistema operativo Linux: Operador, Administrador e introducción a manejo de redes Linux.



LINUX AVANZADA Dirigida a aquellas personas que deseen incrementar los conocimientos del sistema operativo Linux incorporando conceptos tales como: Curso de Redes Avanzado y de Seguridad y Contra-Seguridad de un Sistema Operativo Linux.



LINUX EXPERT Permite la especialización del profesional en un área específica por medio de la realización de distintos workshops sobre temas puntuales, tales como: VPNs, Squid, Firewalls, PHP, Servidores.



Network STORAGE

Marisabel Rodríguez Bilardo
Ing. en Electrónica

El mercado actual ofrece una gran variedad de opciones de equipos y esquemas de implementaciones de Network Storage. Dado el alto costo de los equipos, es necesario saber bien las posibilidades antes de decidir.

El objetivo principal del Network Storage es poner a disposición de los usuarios y las aplicaciones en cualquier lugar de la red y en cualquier momento todos los datos almacenados, tengan el volumen que tengan.
El mismo paso del tiempo hace que la cantidad de información que manejan las organizaciones crezca cada año, y que se necesite tecnología que permita ordenarla y ponerla a disposición de los usuarios rápidamente.
Los modelos de storage fueron evolucionando desde hace mucho tiempo, para lograr que grandes volúmenes de datos puedan administrarse, protegerse centralizadamente y distribuirse entre los servidores y usuarios. Además, las nuevas tecnologías, permiten alivianar el tráfico de las redes corporativas, consumiendo solamente ancho de banda dedicado para eso, lo cual mejora la respuesta de la red en su totalidad.
NAS y SAN compiten actualmente por ser "la" tecnología de Network Storage, pero a medida que pasa el tiempo, las diferencias están destinadas a desvanecerse para que surjan nuevos estándares como SCSI sobre IP y Open Strorage Networking (OSN). Varias empresas como Amdahl, Network Appliance, Cisco, Foundry, Veritas y Legato, están trabajando para combinar lo mejor de las dos tecnologías y lograr una solución correcta para la administración de grandes cantidades de datos.

NASs y SANs

La mayoría de la gente diferencia a las NASs de las SANs por las conexiones y el cableado, pero la diferencia en los protocolos utilizados es el factor más importante. Si comparamos una y otra tecnología, vemos que las NASs usan TCP/IP (Ethernet), FDDI, ATM, y puede ser algún día TCP/IP sobre Fibre Channel, y las SANs se implementan primordialmente con Fibre Channel.
Con respecto a los protocolos, las NASs usan TCP/IP, NFS, CIFS, HTTP, mientras que las SANs usan SCSI encapsulado.
El overhead de TCP/IP baja la eficiencia de la transferencia de datos: una red de 100Mbps tiene un throughput de 60-80Mbps, por eso por lo general se prefiere SCSI por ser más rápido que Ethernet y por lo tanto mejor, pero mientras que la velocidad de SCSI puede llegar a mejorarse al doble en una próxima versión, las velocidades en Ethernet se multiplican por 10, entonces en un futuro cercano puede superar a SCSI.
Network Storage se trata básicamente de guardar



El Sistema HARDkey.NET es una poderosa herramienta para protección de software, cifrado de datos y control de acceso a aplicaciones o sitios de Internet que le permitirá defender eficazmente su inversión de desarrollo, con la mejor relación costo-beneficio, el mismo está basado en llaves electrónicas.

La mejor opción para protección de sus desarrollos

HARDkey.NET se adapta a sus necesidades, permitiéndole elegir entre varios modelos de llaves: para puerto paralelo o USB, monousuario y para compartir en red, con límite de usuarios concurrentes configurable por el desarrollador.

Protección de Software y Datos

Con el sistema HARDkey se puede utilizar dos metodos distintos de protección, uno automático que permite protejer ejecutables ya compilados y el otro invocando a librerías desde el código fuente. El entorno de protección automática de ejecutables le brinda la opción de especificar qué archivos asociados a ese programa se desean manejar en forma cifrada para que la información en disco sólo pueda ser accedida por el ejecutable protegido con HARDkey.



Llave de protección con RTC

Este modelo posee un reloj de tiempo real que permite controlar la fecha de vencimiento de una licencia de uso en forma independiente del reloj de la PC. Con esto el desarrollador logra armar un esquema de alquiler o leasing seguro ya que el usuario final del sistema no puede alterar el reloj de la llave para extender el uso de una licencia vencida.

Autenticación de usuarios

Además de la aplicación tradicional de protección de software, las llaves HARDkey USB pueden utilizarse para implementar una autenticación de acceso a las aplicaciones mediante dos factores, **algo que tengo** (la llave) más **algo que sé** (un pin).
Esto pemite cumplir con normas de seguridad como la ISO 17799.



datos usando un método que permita que estén disponibles en una red. A través de los años, el resguardo de los datos pasó por varias etapas, sobre todo porque el volumen de información a guardar ha ido creciendo paulatinamente, lo que favoreció el surgimiento de tecnologías y arquitecturas para solucionar los problemas que esto trae aparejado. En los tiempos de los mainframes, los datos se guardaban separadamente, no dentro de la unidad de procesamiento. Cuando las computadoras estuvieron más al alcance de los usuarios, los dispositivos de storage se ubicaron dentro de las mismas, o en cajas externas que se conectan directamente al sistema. Con el crecimiento del volumen de datos a guardar, se necesitaron otras alternativas que facilitaran el acceso y que fuesen cada vez más rápidas.

DAS (Direct Attached Storage):

Se llama así al método por el cual el dispositivo de storage está directamente conectado a un servidor. El ejemplo más simple de DAS es el disco rígido de una computadora. También entran dentro de esta categoría los discos que se conectan directamente al sistema, aunque sean externos. Es el método más usado en las computadoras hoy en día.

NAS (Network Attached Storage):

Es el mecanismo por el cual se conectan servidores especiales de storage a la red. Estos dispositivos tienen una dirección IP asignada y se puede acceder a ellos a través de un servidor que actúa como gateway para los datos, o en algunos casos, permite compartir datos directamente sin intermediarios. (Ver Figura 1).

La ventaja de la estructura de NAS es que varios servidores con sistemas operativos diferentes se pueden conectar centralizadamente, lo que permite asegurar y administrar los datos de una manera más efectiva. Otra ventaja de las NASs es que se puede expandir el storage disponible con mucha facilidad. Alcanza con agregar otro dispositivo.

Las NASs también agregan otro nivel de "fault tolerance" (tolerancia a fallos) a la red con respecto a DAS, porque si llega a pasarle algo a un servidor, con una NAS los datos van a seguir siendo accesibles por todos los clientes de la red. Para asegurarse de que la NAS no es otro punto de falla, es recomendable utilizar algún tipo de RAID.

SAN (Storage Area Network):

Es una red de dispositivos de storage que se conectan entre sí y a un servidor o Cluster de servidores que actúan como puntos de acceso. En algunas configuraciones, la SAN también está conectada a la red. Se utilizan switches que actúan como puntos de conexión de la SAN. El hecho de que la red de storage esté separada de la LAN hace que todo el caudal de información que se transfiere no consuma ancho de banda de los clientes. Esta es una de las razones por las cuales las compañías eligen tener una SAN. (Ver Figura 2).

El tema principal al momento de elegir la tecnología de Network Storage es el precio, e implementar una SAN tiene un costo asociado muy alto.

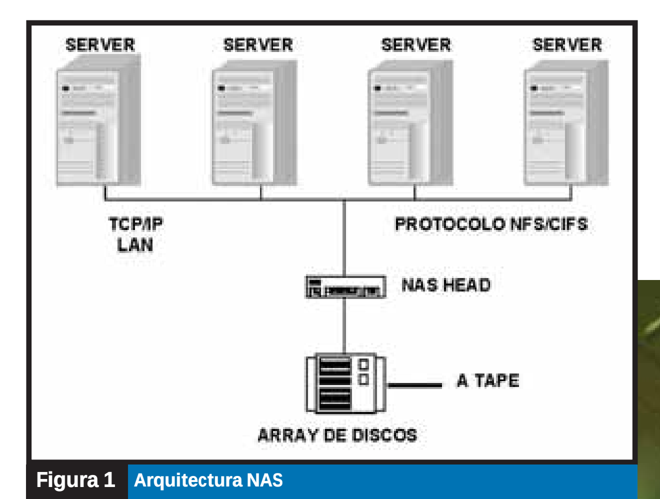


Figura 1 Arquitectura NAS

Básicamente, una SAN es un conjunto de servers en una red, accediendo a un pool central de storage. Conceptualmente una SAN se puede pensar como una red separada de dispositivos de storage conectados a a la red LAN. Las SAN permiten que el tráfico de storage esté fuera de la LAN, creando una red separada diseñada específicamente para datos.

Las SANs representan un paso en la evolución de la tecnología de storage. Tradicionalmente, en los sistemas cliente-servidor, los datos se guardaban en dispositivos internos o directamente conectados a los servidores. El próximo paso en la escala evolutiva del storage fueron las NASs, en donde se conectaron los dispositivos de storage fuera de los servidores, directamente a la red. Las SANs toman este principio y lo llevan más allá: los dispositivos de storage tienen su red separada y se comunican directamente entre sí a través de redes mucho más rápidas. Los usuarios tienen acceso a ellos utilizando los "Storage Servers" que se conectan tanto a la LAN como a la SAN. Utilizar la LAN para dar servicios de storage es una estrategia que limita el ancho de banda total de la red. Las SANs absorben todo el ancho de banda utilizado para el resguardo de datos y los cuellos de botella asociados con la LAN y las limitaciones de escalabilidad que tienen las implementaciones basadas en buses SCSI.

Las ventajas de las SANs son muchas, pero una de las mejores es el backup sin servers ("Server-Less Backup"). Este sistema permite a un dispositivo de storage copiar datos directamente a un disco de backup a través de links de alta velocidad de la SAN sin intervención del servidor. Los datos se guardan en la SAN, lo que significa que la transferencia no toma ancho de banda de la LAN, y los recursos de procesamiento del servidor quedan disponibles para los requerimientos de los clientes.

Más allá de que usemos DAS, NAS o SAN, hay varias tecnologías que utilizan los 3 tipos de red, como por ejemplo SCSI y RAID. Por años se utilizó SCSI par transportar datos en forma confiable y rápida. A través del tiempo evolucionó y actualmente es la tecnología más utilizada. RAID (Redundant Raid of Independent Disks) es una serie de estándares que brindan performance mejorada y tolerancia a fallos.

Las SANs se implementan utilizando Fibre Channel, que llega a transferir 2Gbps (se prevé que esté disponible en un corto plazo con velocidad de 4G, a un precio similar). Se puede usar en una configuración punto a punto entre dos dispositivos o también en forma de anillo. Se utiliza un switch de Fibre Channel que básicamente funciona como un switch para Ethernet, y actúa como punto de conectividad entre los servidores. Como es una tecnología switcheada, provee un camino





Figura 2 Arquitectura SAN

dedicado y libre de colisiones para la transferencia de datos.
Las aplicaciones que requieren transferencias de grandes cantidades de datos, son las candidatas principales para utilizar una SAN. Pueden ser: backup, replicación de datos, protección ante desastres, "Data Warehousing", comercio electrónico, broadcasting, geografía, entre muchas otras.
Para proteger datos efectivamente en una SAN, se necesitan algunos elementos:
- *Administración centralizada*
- *Soporte para compartir bibliotecas removibles*
- *Backup "LAN-Less" y "Server-Less"*
- *Soporte para plataformas heterogéneas*
- *Mirroring remoto*
- *Backup Real-Time*
- *True Data Sharing*

Administracion centralizada
Idealmente, una consola central tendría que manejar todos los recursos físicos de storage en una red de una empresa.
Debería haber una consola que automáticamente guarde y analice la configuración de capacidad, uso de espacio e información de performance de todos los recursos de storage. Los recursos lógicos monitoreados incluyen file systems, directorios, archivos y repositorios específicos de aplicaciones.
Los recursos físicos de los que se puede hacer un seguimiento incluyen RAIDs, bibliotecas de cintas ("Tape libraries"), entre otros. Casi todos los proveedores ofrecen administración centralizada, los líderes en este área son Veritas, Legato, Computer Associates (CA), y también IBM.

Soporte para bibliotecas removibles
Por lo general cuando se hacen backups, se resguardan los distintos servers localmente, utilizando grabadoras de cintas ("tape drives") directamente conectadas. Un beneficio de las SANs y de las NASs, es la habilidad de compartir recursos (por ejemplo una biblioteca de cintas) entre muchos servidores de backup. Los recursos compartidos permiten a los administradores consolidar los backups en una sola biblioteca.
Sin embargo, esto no significa solamente compartir el acceso al espacio en cintas, sino también la instrumentación de la administración óptima del espacio. Administrar una biblioteca significa manejar el acceso a los medios y la determinación dinámica de los drives a utilizar en cada momento entre los distintos servidores, de tal forma que cualquier servidor siempre tenga disponible algún drive para escribir.
En muchos casos, la posibilidad de conectarse a la biblioteca con distintos servidores a través de la SAN justifica comprar un software de automatización.
Un proveedor a un precio razonable de esta tecnología es Hierarchical Storage Management (HSM), Legato, Veritas, CA, y Seagate son líderes en este rubro, junto con Avalon de EMC, que soluciona implementaciones complejas con cachés de arrays de Discos y Bibliotecas de cintas ("Tape Libraries").

LAN-Less y Server-Less backup
Actualmente los esquemas de backup evolucionados y que manejan mucha información, se realizan en 3 fases. La primera etapa consiste en mover los datos desde el disco hacia el servidor directamente conectado, y a través de la LAN hacia otro servidor que enviará los datos a cinta cuando corresponda. En la segunda fase, la SAN permite realizar el backup fuera de la LAN. Los datos se mueven de un disco al servidor, el que retransmite la información hacia la Biblioteca ("Tape Library") de la SAN. En la tercera etapa, el servidor inicia el comando de backup. Los datos se mueven directamente de disco a cinta, a través de la SAN sin involucrar al servidor. Esta configuración se llama "Server-Less" Backup. Intelliguard es una de las marcas que adquirió Legato recientemente, y está desarrollando esta tecnología.

Soporte de plataformas heterogéneas
Las primeras implementaciones de las SAN fueron generalmente para una plataforma homogénea. A medida que pasó el tiempo, fue más común contar con entornos heterogéneos, por lo tanto un buen software de administración necesita la capacidad de controlar equipos de distintos proveedores y distintas bases de datos o file systems, resguardando los datos en cualquier biblioteca de cintas o array de discos, también utilizando cualquier switch o hub, router o bridge. EMC y Veritas son ejemplos de proveedores que soportan este tipo de esquema de múltiples plataformas.

Mirroring remoto
Las distancias de conexión que permite Fibre Channel son de alrededor de 10 a 20 km, dependiendo del uso, esto permite facilitar el acceso a los sitios remotos para backup o recuperación ante desastres. Las SANs también pueden conectarse a WANs para lograr niveles adicionales de conectividad y protección. Comm Vault es uno de los vendedores que ofrecen aplicaciones de este tipo. CNT ofrece implementaciones de conectividad SAN a WAN con SCSI y ESCON (Enterprise Systems Connectivity), y también están desarrollando soporte para Fibre Channel.

Backup en RealTime
La importancia de este tipo de backup (también llamado Window-Less backup o Hot Backup), se hace obvia cuando nos enfrentamos a un volumen de datos considerable en una SAN. El backup en Real-Time, esencialmente permite resguardar un volume o file system periódica y automáticamente, sin afectar la operación normal del sistema. La técnica más usada se llama "snapshot", en donde se copian los datos cuando se accede y modifica el volumen original en operaciones nor-

males. Varias marcas están desarrollando productos para lograr Network Integrity (así se llama el esquema), como por ejemplo EMC y HDS. Los mayores proveedores de soluciones de backup total son ADIC, ATL, StorageTek (ahora comprado por Sun Microsystems), Hewlett-Packard, Exabyte, y Overland.

True Data Sharing
(Disponibilidad de datos verdaderos)
Cuando se comparten datos sin hacer una copia, y muchas computadoras de diferentes plataformas pueden acceder a la misma instancia física de datos guardados en un subsistema de storage, estamos utilizando "True Data Sharing". Hay muchos niveles de complejidad de esta tecnología, y muchos tipos de implementaciones. El primer nivel es cuando computadoras de plataformas disímiles acceden a los datos, pero solo el dueño original de los datos puede modificarlos. El segundo nivel es cuando distintas computadoras con distintas plataformas pueden reescribir y agregar datos, pero uno a la vez. En este caso debe haber un mecanismo de locking para prevenir momentáneamente las superposiciones. El tercer nivel se llama "Concurrent Data Sharing" (para compartir concurrentemente), y permite que cualquier plataforma escriba o agregue datos en cualquier momento. Hay muchas ventajas utilizando este esquema. Con una sola copia de los datos, no se necesita hacer replicaciones, lo que simplifica el mantenimiento, eliminando los problemas de sincronización. "True Data Sharing", a través de distintas plataformas con distintos sistemas operativos requiere traducir a un sistema operativo común la administración de la transferencia de datos. Algunos proveedores son: Sequent, Mercury Computer Systems, DataDirect, Transoft, Retrieve, y Network Disk. Para una arquitectura NAS: NetApp, EMC, Sun, IBM, y Procom .

Algunas de las Tecnologías Involucradas

Infiniband
Es un bus serial de alta velocidad, diseñado para conexiones internas y externas. Originalmente se pensó como una tecnología que conectase

-------- NAS --------	-------- SAN --------
En una NAS, cualquier máquina que se conecte a la LAN va a poder acceder a los archivos compartidos.	*Solamente los dispositivos que posean Fibre Channel SCSI pueden conectarse a la SAN. El Fibre Channel tiene como máximo 10Km de largo.*
En una NAS se identifica la información por el nombre de archivo y los offsets o metadata, y también soporta autenticación de usuarios y permisos.	*Una SAN direcciona la información por número de bloque y transferencia.*
Una NAS permite compartir un mayor volumen de información especialmente entre sistemas operativos distintos como Unix y Windows.	*Compartir archivos depende del sistema operativo.*
La NAS "head unit" maneja el file system.	*Los servidores manejan el file system.*
Los backups y mirrors se realizan sobre los archivos, no por bloques, para ahorrar ancho de banda y tiempo.	*Los backups and mirrors requieren una copia block por block, a pesar de que los bloques estén vacíos. Un dispositivo que hace mirror debe tener una capacidad igual o mayor comparada con la de origen.*

CPUs a una velocidad muy alta de I/O. En este punto, podría reemplazar a los estándares de I/O como PCI o Fibre Channel, y algunas redes como Ethernet. Esta tecnología conectaría todos los CPUs y periféricos a una matriz única de Infiniband. Esta visión tiene muchas ventajas además de la velocidad, porque se separa la carga de trabajo de los buses de los servidores. En teoría, debería permitir la construcción de clusters más fácilmente, y además potencialmente más baratos, porque se pueden compartir más dispositivos a alta velocidad, ya que la carga de trabajo se distribuye.
Muchas implementaciones utilizan protocolos estándar como PCI para las conexiones locales, y usan Infiniband para realizar interconexiones entre servidores.
Hoy en día se utiliza principalmente para aplicaciones de clusters.

iSCSI
El protocolo iSCSI utiliza TCP/IP para transferir datos. A diferencia de otros protocolos de Network Storage como Fibre Channel (que es el fundamento de la mayoría de las SANs), requiere solamente una interfaz Ethernet para operar, lo que permite bajar los costos de la centralización del storage, sin sufrir incompatibilidades como con Fibre Channel.
Una desventaja de iSCSI surge de comparar la velocidad con Fibre Channel, porque con respecto a éste, agrega un overhead considerable cuando realiza la comunicación entre los clientes y el servidor de storage. Sin embargo hay nuevas técnicas como TCP Offload Engine (TOE) que ayudan a reducir este overhead. iSCSI ha sido ampliamente testeado y demostró que tiene una performance excelente en SANs, probando tanto con TOEs como con tarjetas Gigabit Ethernet.

Network Storage hoy

Muchas son las opciones y los proveedores, pero de todas formas todavía es muy caro armar una red de storage. Las tendencias llevan a aumentar la velocidad de los buses y abaratar el precio del GigaByte en el mercado. Hay productos muy nuevos que permiten tener conexiones Ethernet para discos rígidos a menos de u$d1.35 el GigaByte, o Tape Libraries con miles de GigaBytes de capacidad, pero falta mucho para que termine la pelea por ganar el mercado y estandarizar un protocolo único para las Storage Networks.



CONFIGURACIÓN E IMPLEMENTACIÓN

Nuestro primer acercamiento al interior de una Soft PBX con ASTERISK

Alejo Gagliardi

En la publicación anterior sobre ASTERISK (nex#21, pág. 58) realizamos una introducción al mundo de la telefonía IP y, en particular, a las características mas relevantes de esta completa Soft PBX. Vimos también los protocolos y codecs que soporta y que clase de dispositivos o software cliente se le podía conectar a través de los mismos.

En este artículo nos introduciremos en las minucias del ASTERISK, veremos su organización y por último veremos la configuración básica de una PBX a modo de punto de partida. Ésto es sólo la punta del iceberg pero es un buen comienzo para todos aquellos que luego deseen ponerse manos a la obra y profundizar en el mundo de ASTERISK.

Obteniendo e instalando el código fuente.

Dependiendo de la distribución de Linux que estemos usando seguramente vamos a encontrar paquetes precompilados de ASTERISK, por ejemplo rpms en el caso de Fedora, si bien estos paquetes son mas fáciles de instalar, por lo general no poseen la ultima versión del software, y como ya dijimos, son para una distribución de Linux en particular, por lo que vamos a optar por realizar el proceso desde cero, esto implica obtener el código fuente y compilarlo en nuestro Linux.

Antes de obtener y compilar el ASTERISK tenemos que cumplir con los siguientes prerrequisitos: *ncurses*, *openssl* y *zlib*, con sus respectivos -devel, cómo así también *bison*, sólo para versiones 1.0.X de ASTERISK, con su correspondiente -devel.

Una vez cumplido los prerrequisitos vamos obtener el código fuente de ASTERISK, la versión del mismo al momento en que se escribió este artículo es la 1.2.1, la dirección desde la cual podemos bajar los archivos es: http://www.asterisk.org/download.

En esta página Web encontraremos varios archivos para bajar para nuestro artículo; sería suficiente con bajar y compilar: http://ftp.digium.com/pub/asterisk/asterisk-1.2.1.tar.gz

En caso de que necesitemos usar hardware especializado para utilizar líneas analógicas y/o digitales también vamos a necesitar los siguientes archivos: http://ftp.digium.com/pub/zaptel/zaptel-1.2.1.tar.gz; http://ftp.digium.com/pub/libpri/libpri-1.2.1.tar.gz

Si bien nosotros a los fines de este artículo sólo necesitamos *asterisk-1.2.1.tar.gz*, vamos a compilar los tres a modo de ejemplo. Una vez que tenemos bajados los archivos los copiaremos al siguiente directorio; no es estrictamente necesario que sea este directorio pero es un buen lugar para ubicarlos:

```
/usr/local/src
```

Luego hacemos:

```
# cd /usr/local/src
# tar -vxzf  zaptel-1.2.1.tar.gz
# tar -vxzf  libpri-1.2.1.tar.gz
# tar -vxzf  asterisk-1.2.1.tar.gz

# cd zaptel-1.2.1
# make
# make install

# cd libpri-1.2.1
# make
# make install

# cd asterisk-1.2.1
# make
# make install
# make samples
```

Esto último generará un conjunto de archivos de configuración de ejemplo en el directorio /etc/asterisk, cuyo significado analizaremos más adelante en este artículo, se debe tener cuidado ya que si ya teníamos archivos de configuración en esta carpeta de una instalación previa éstos serán remplazados con los de ejemplo y perderíamos cualquier configuración que hayamos realizado.

La compilación, si es que se van a compilar las bibliotecas de zaptel y libpri, se debe realizar respetando el orden en le que están en el ejemplo más arriba por una razón de dependencias.

Una vez realizado el proceso de compilación anterior y si nada nos dio error, ya tenemos el ASTERISK instalado y listo para funcionar. Como se puede observar el proceso de instalación es muy simple. Para comprobar que todo funciona como corresponde iniciaremos el ASTERISK con el siguiente comando:

```
# asterisk -vvvc
```

La opción -vvv nos muestra información de depuración y la opción -c indica a ASTERISK que nos inicie una consola, por lo tanto si todo salió bien deberíamos ver:

```
# CLI>
```

Ésto indica que el ASTERISK esta funcionando correctamente. Para detener el ASTERISK escribimos lo siguiente:

```
# CLI> stop now
```

En /etc/asterisk donde están los archivos de configuración de ejemplo que trae el ASTERISK que fueron creados mediante el comando *make samples* encontraremos varios archivos que son los que manejan el comportamiento del ASTERISK por completo. Estos archivos poseen todos una estructura similar y cuentan con una sección GENERAL donde se realizan las configuraciones comunes. Puede además poseer una o más secciones cuyo propósito y nombre variará según el archivo de configuración; los valores se asignan con el formato de <clave>=<valor>.

Si bien son varios archivos, nosotros centraremos nuestra atención principalmente sobre los denominados extensions.conf y sip.conf debido a que son lo que utilizaremos en nuestro ejemplo más adelante.

Primero lo más importante: el Dial Plan

El más importante de todos estos archivos de configuración es el denominado *extensions.conf* el cual es el corazón del ASTERISK ya que es el que posee el plan de discado o *dial plan*, o sea que es el que controla el flujo y ejecución de todas las operaciones del ASTERISK, por ejemplo cómo tienen que ser manejadas y ruteadas todas las llamadas entrantes y salientes por lo cual vamos a verlo con un poco más de detenimiento.

Este archivo posee dos secciones en su comienzo que pueden o no estar presentes. La primera es [*general*] que es donde se realizan unas pocas configuraciones con referencia al plan de discado, luego le sigue la sección [*globals*] que es donde se realiza la definición de constantes o variables globales al plan de discado y su valor inicial. La parte restante por debajo de la sección [*globals*] es el plan de discado propiamente dicho el cual está compuesto por un conjunto de contextos, los cuales a su vez contienen un conjunto de extensiones.

Un contexto es simplemente un una sección que identifica o "contiene" un conjunto de extensiones. Los contextos son importantes para implementar características como seguridad, ruteo, preatendedores, menús multinivel, macros, etc.

Las extensiones son las que indican que hacer dada una determinada condición, como por ejemplo ser el número que se discó. Un ejemplo para graficar sería:

```
[default]

exten => 1234 ComunicarConVentas
```

En este ejemplo dentro del contexto "default" tenemos la extensión 1234, si alguien disca este número el ASTERISK nos comunicará con el sector Ventas. Éste es un ejemplo para graficar, en la realidad la sintaxis es similar.

Las extensiones pueden tener varios pasos o prioridades y son de la forma:

```
exten => <exten>,<prioridad>,<aplicación(argumentos)>
```

El flujo de la llamada continúa a través de la extensión ejecutando las aplicaciones secuencialmente hasta que no halla más pasos dentro de la extensión o bien alguna aplicación devuelva -1. Un ejemplo real sería:

```
exten => 1234,1,Wait(1)
exten => 1234,2,Answer
```

Aquí 1234 es la extensión, 1 y 2 son las prioridades o pasos, y Wait y Answer las aplicaciones

La comparación de la extensión puede ser un número definido como en el ejemplo anterior o bien mediante una plantilla, ésto se indica mediante el caracter "_" y la comparación se realiza a través de caracteres comodín:

-N: un único dígito entre 2 y 9

-X: un único dígito entre 0 y 9

-[1-4]: un único dígito que coincida con cualquiera de los especificados entre corchetes

-. : cualquier número

Las siguientes son extensiones especiales que son usadas por ASTERISK:

s - En esta extensión se tratan todas las llamadas que no posean una extensión definida.

i - En esta extensión se tratan las llamadas cuya extensión es inválida.

t - En esta extensión se tratan las llamadas que dieron Time out.

o - Extensión de operador.

Los canales

Para completar el conjunto de elementos que componen la estructura básica del ASTERISK queda mencionar los canales. Los canales son las conexiones al ASTERISK que se convierten en llamadas. Los tipos de canales más comunes son:

-**Zaptel** (para líneas analógicas)

-**IAX** (para conexiones IP a través de IAX)

-**SIP** (para conexiones IP a través de SIP)

Cada uno de estos canales posee un archivo diferente de configuración en el cual se le definirá el comportamiento a cada uno. Lo que tienen en común los canales es que deben tener definido a que contexto del plan de discado están asociadas las llamadas que por ellos ingresen, de esta forma el ASTERIK sabrá como tratar las mismas.



Poniendo todo junto

Ahora que conocemos la estructura básica de los elementos que componen el ASTERISK y sus principales archivos de configuración, podemos resumirlo de la siguiente manera: cuando el ASTERISK recibe una llamada a través de uno de sus canales, esa llamada pertenecerá a un contexto determinado, que es el que se definió en el archivo de configuración del canal en cuestión, de esta manera el ASTERISK buscara ese contexto en el plan de discado y tratará la llamada según las directivas que posean las extensiones definidas dentro de ese contexto.

Como podemos ver, la forma más común de usar un contexto es para indicarle al ASTERISK que hacer con una llamada dependiendo de dónde provenga la misma, por ejemplo, se puede tener un contexto para las llamadas que ingresan por las líneas analógicas, en el cual se instruye al ASTERISK que reproduzca un mensaje de bienvenida y se pida el interno con el que se quiere comunicar, y otro contexto para los números internos de la central en el cual se instruya al ASTERISK que si la llamada que se quiere realizar es una llamada de larga distancia, le solicite una clave de identificación al usuario. La flexibilidad que provee el uso de contextos nos permite tener un control muy fino sobre las acciones que realizará el ASTERISK con una llamada dependiendo de donde se haya originado la misma.

La comprensión del plan de discado, su estructura lógica y la interacción de éste con los canales constituye la base para poder realizar cualquier implementación. A continuación vamos a poner todo lo visto anteriormente en un ejemplo básico integrador que seguramente clarificará y fijará los conceptos descriptos en los párrafos anteriores

Mi primer Soft PBX

Bien, es hora de arremangarse y poner manos a la obra; la idea de este ejemplo es configurar el ASTERISK para poder conectar dos **Soft Phones** a modo de internos, en nuestro caso utilizaremos el **SJPhone** que ustedes pueden obtener de la siguiente dirección: *http://www.sjlabs.com/SJphoneWin/* . A los efectos de poder montar este ejemplo necesitaremos tres computadoras, una con Linux y ASTERISK instalado y otras dos con Windows con el SJphone instalado. El SJphone soporta H323 y SIP, nosotros en el ejemplo usaremos SIP ya que el soporte H323 no viene por defecto en el ASTERISK y debe ser compilado por separado.

Las tres computadoras están en la misma red; en nuestro experimento usaremos la red 192.168.0.0/24 y asignaremos las IP de la siguiente manera:

Linux: 192.168.0.100/24

Win1: 192.168.0.101/24

Win2: 192.168.0.102/24

Una vez que poseemos el escenario montado y el ASTERISK funcionando pasaremos a configurarlo. Lo primero que haremos es configurar el plan de discado, para ello remplazaremos el archivo *extensions.conf* que ASTERISK instala como ejemplo por uno con el mismo nombre que contenga:

```
extensions.conf

[general]

static=yes   ; Estas dos líneas son para prevenir
writeprotect=yes ; la sobre escritura del plan de discado

[globals]

[telefonos-sip]

exten => 1234,1,Dial(SIP/1234)
exten => 1235,1,Dial(SIP/1235)

exten => i,1,Play(invalid)
```

En el archivo *extensions.conf* en la línea

```
exten => 1234,1,Dial(SIP/1234)
```

Estamos diciendo que si alguien disca la exten-

sión 1234 el ASTERISK debe llamar a esa extensión por lo que si alguien disca 1234 el SJphone con esa extensión comenzara a hacer ring.

exten => i,1,Play(invalid)

en esta línea le decimos al ASTERISK que si alguien disca una extensión que no este definida en el plan de discado le reproduzca una archivo de sonido que le avisara al usuario que disco una extensión inexistente.

Hacemos lo mismo con el archivo *sip.conf*

sip.conf

```
[general]
port = 5060           ;puerto en el que va a escuchar el asterisk
bindaddr = 0.0.0.0    ;IP en la que va a escuchar, en este caso
                      ;0.0.0.0 indica en todas las IP

context = telefonos-sip   ;contexto por defecto

[1234]                ; teléfono sip 1234
type=friend
username=1234
secret=1234
canreinvite=no
host=dynamic
dtmfmode=rfc2833
nat=yes
allow=all

[1235]                ; teléfono sip 1235
type=friend
username=1235
secret=1235
canreinvite=no
host=dynamic
dtmfmode=rfc2833
nat=yes
allow=all
```

En el archive *sip.conf* definimos las entradas donde que van a validar nuestros Soft Phones, a continuación una explicación de cada línea.

type=friend

Significa que este cliente puede hacer y recibir llamadas.

secret=1235

Clave que deberemos poner para registrarnos en el ASTERISK

canreinvite=no

nat=yes

Estas líneas son para acomodar los mensajes de SIP para solucionar problemas relacionados con el NAT (Network Address Translation).

host=dynamic

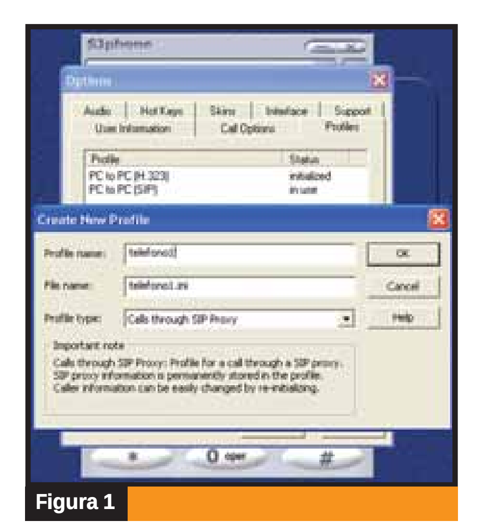


Figura 1

esta línea informa que el cliente, en este caso nuestro Soft Phone, puede tener IP dinámica.

dtmfmode=rfc2833

En esta línea configuramos el modo en que se enviarán al ASTERISK los tonos de discado.

allow=all

En esta línea activamos el uso de todos los codecs de los que dispone el ASTERISK, ésto no significa que vaya a usar todos al mismo tiempo, sino que ASTERISK elegirá el más conveniente para trabajar con el cliente.

Una vez realizado ésto iniciamos el asterisk como lo hicimos la primera vez para probarlo con el comando

asterisk -vvvc

Ahora sólo nos queda la configuración de los Sjphone.

Abrimos el SJphone y hacemos click con el botón derecho de Mouse y elegimos *Options* del menú se nos desplegará una ventana con el título Options, en la que seleccionamos la ficha denominada *Profiles* y hacemos click en el botón denominado *New* para crear un nuevo perfil. Nos aparecerá una ventana con el título "Create new profile" y en el cuadro de texto denominado Profile Name ingresamos el nombre del perfil, en este caso le ponemos telefono1, el resto debe quedar por defecto (Profile file = telefono1.ini y Profile type=Call through sip proxy) como vemos en la figura 1. A continuación hacemos click en el botón **OK** y nos a parecerá la pantalla que vemos en la Figura 2.

Elegimos la ficha denominada SIP Proxy y completamos el cuadro de texto denominado Proxy domain con la IP del ASTERISK en este caso 192.168.0.1 y a continuación completamos el cuadro de texto que se encuentra a la derecha del que acabamos de completar, que posee un cero, lo reemplazamos por 5060 que es el puerto que configuramos en el *sip.conf* y es donde ASTERISK aceptará el registro de los clientes.

Hacemos click en el botón "**OK**" y nos aparecerá una ventana en la que deberemos ingresar la cuenta y la clave para el registro (Figura 3).

Aquí completaremos Account con el número que pusimos en la definición del *sip.conf* (en este caso era **[1234]**) y en el campo Password ponemos lo que configuramos como secret en el *sip.conf* (en nuestro caso **secret**=*1234*).

Hacemos click en OK y volveremos a la pantalla de Opciones, donde volvemos a hacer click en OK y de esta forma terminamos la configuración del primer SJphone el cual nos informara en letras blancas si se ha podido registrar o no.

Por una cuestión de simplicidad solo haré al configuración para la primera extensión. Para la segunda es lo mismo tan sólo deben remplazar el número de cuenta y clave por los de la segunda en nuestro caso **Account**=*1235* y **Password**=*1235* y por una cuestión de prolijidad deberíamos poner **Profile name** = *telefono2*.

Al terminar cada configuración de cada Soft Phones deberíamos ver un mensaje de registración en la consola del ASTERISK.



Figura 2

Nuestra primer llamada.

En este momento esta todo configurado y funcionando con lo que si desde el SJphone denominado *telefono2* disco 1234 y hago click en el ícono que es un pequeño teléfono verde debería comenzar a hacer ring el **SJphone** denominado *telefono1*, para atender la llamada basta con hacer click en el ícono que es un telefonito verde del **Soft Phone** que esta sonando y se habrá establecido la comunicación.

Si bien éste es un ejemplo muy básico es el "Hello World" de las configuraciones que sirve de partida para comenzar con el mundo de ASTERISK; espero disfruten investigando.



Figura 3

Metasploit Framework

Hernán Marcelo Racciatti
Senior Security Consultant - SIC Informática

Metasploit Framework, no es más que otra prueba respecto de que el software libre puede dotar a la comunidad de proyectos de calidad. Invierta unos minutos en la lectura del presente artículo y comprenda porque Metasploit Framework es una herramienta que no debe dejar de conocer.

Hace algunas semanas, me encontraba dictando un workshop dirigido a algunos de los integrantes del Team de seguridad de una importante empresa extranjera, cuando a partir de una pregunta surgida respecto del tema acerca del cual estaba exponiendo, comenzaron a salir de mi boca palabras tales como: "Red Teaming Process", "0 Day", "Exploit", "Shellcode", "Automated Penetration Testing Tools", "Metasploit" y algunas otras que no recuerdo en este momento... Si bien es cierto, que cada una de estas palabras surgía con total naturalidad de mis labios, también lo es el hecho que luego de algunos instantes comencé a notar que los asistentes parecían tener alguna dificultad para entender o interpretar algunos aspectos de mi respuesta.

Tal como es mi costumbre, atento a clarificar cualquier duda que pudiera existir, interrumpí la oratoria, escribí las palabras sobre las cuales podía existir dudas en una pequeña pizarra que amablemente me facilitaron, y pregunte si todos conocían el significado o al menos la existencia de las mismas. Para mi sorpresa, a pesar de la vasta y probada experiencia en seguridad informática que poseían, la mayor parte de los asistentes nunca había oído mencionar dichas palabras, y tan solo algunos creían haber leído acerca de estos temas en alguna oportunidad.

Como no podía ser de otro modo, dedique algunos minutos para explicar cada uno de los términos, me asegure que al menos los conceptos principales queden claros y continué con el tema especifico que nos había reunido aquella tarde.

Sucede que a menudo, la formación del profesional de seguridad tradicional, no incluye más aspectos que los estrictamente formales, lo cual generalmente significa dejar de lado, una parte importante de recursos, tácticas, herramientas o al menos un punto de vista distinto respecto de la seguridad.

Ahora bien, probablemente usted sea un prestigioso profesional tal como las personas que participaron de mi charla, con muchos años de experiencia en especialidades tales como: seguridad gerenciada, control de acceso, seguridad física, administración de firewalls, seguridad en redes, sistemas operativos o cualquier otra actividad relacionada con la seguridad de la información, pero al menos que sea un persona dedicada a específicamente a realizar evaluaciones de seguridad, o un entusiasta con el tiempo, interés y dedicación necesaria como para investigar mas allá de lo mencionado en los libros, tal vez desconozca al igual que las personas mencionadas en los párrafos anteriores, la existencia de algunos conceptos u herramientas que los atacantes (o quienes tienen a su cargo la responsabilidad de realizar test de intrusión controlados) utilizan a diario con una facilidad digna de admiración.

Dicho esto, mi intención al escribir el presente artículo no es la de extenderme en detalles técnicos (Aunque podría aparecer alguno…), sino por el contrario, que el contenido del mismo le permita a usted conocer la existencia de una de las principales herramientas al alcance del profesional al momento de realizar testeos de seguridad controlados, así como también los aspectos básicos necesarios a efectos de su utilización, de modo tal que pueda dar sus primeros pasos con la herramienta presentada, no sin antes conocer algunos de los términos asociados que sin duda resultaran de su interés (Ver "Definiciones en tres líneas...").

Definiciones en tres líneas!

Exploit: A menudo solemos referirnos por el termino "Exploit", al mecanismo por el cual es posible "Explotar!" o aprovecharse de una vulnerabilidad previamente identificada, con el fin de lograr una condición favorable en función del objetivo del ataque. De este modo, dicho mecanismo puede ir desde una pequeña porción de código de programación específicamente diseñado con el fin de aprovecharse de un bug determinado, o el argumento utilizado al momento de lanzar un ataque de ingeniería social.

Shellcode: El termino Shellcode se refiere a un bloque de código binario, capaz de completar una tarea especifica. Dicha tarea puede ir desde la simple ejecución de un comando del sistema, hasta la obtención de una shell del sistema objetivo (De hecho e de aquí su nombre!).

0 Day: Si bien es cierto que en la actualidad es posible encontrar varias acepciones de dicho termino, a menudo suele relacionarse el mismo con aquellos exploits en manos de un reducido grupo de personas, aparecidos antes de que una vulnerabilidad sea reportada o se haga publica. Desde el punto de vista de la seguridad, los 0 Days son vistos como cartas ganadoras, debido a que por lo general millones de sistemas podrían eventualmente ser atacados, antes siquiera de que sus propietarios tengan idea que se encuentran expuestos.

Comenzando desde el principio

Tal como se menciona en su sitio en Internet, Metasploit Framework, es una avanzada plataforma "Open Source", diseñada específicamente con el objetivo de potenciar y agilizar, el desarrollo, testeo y utilización de exploits.
El proyecto relacionado con este framework, que según sus progenitores naciera como un juego, ha evolucionado hasta convertirse hoy día en una herramienta fundamental, dentro del Toolkit del profesional relacionado de uno u otro modo con las tecnologías de seguridad de la información.
Escrita casi íntegramente en "Perl" y con varios componentes desarrollados en "C" y "Assembler", su portabilidad se encuentra asegurada, aspecto que ha contribuido en gran parte a su aceptación masiva, pues cualquiera sea su elección en cuanto a la plataforma a utilizar (Like-Unix, BSD, MacOS X, Windows, etc.), tendrá la posibilidad de instalarlo y disfrutar de toda su potencia en tan solo algunos minutos sin mayores dificultades.
Respecto de su licenciamiento, las ultimas versiones de Metasploit Framewok (Incluyendo Metasploit Framework 3.0 aún en proceso Beta - Ver "En Beta"), se encuentran basadas tanto en GPL v2 como en "Perl Artistic Licenses", permitiendo su utilización tanto en proyectos Open Source como en proyectos comerciales.

Herramientas Automatizadas de Testeo de Penetración

Habitualmente Metasploit suele ser identificado como una herramienta automatizada de testeo de penetración. Si bien es cierto que uno puede coincidir o no con dicha apreciación, la comparación de este framework con productos comerciales tales como Core Impact (Core Security Technology) o Canvas (Immunity Sec) suele ser inevitable. A pesar de ello cada una de estas herramientas posee características distintivas que las hacen únicas en situaciones particulares.

Instalación en Gentoo Linux

1. Actualización del árbol Portage

fiona root # emerge -sync

2. Ejecutando la instalación

fiona root # emerge metasploit

3. Actualizando el framework con los últimos componentes publicados

fiona root # msfupdate -u

Instalación en Windows

1. Descargando Metasploit Framework

http://www.metasploit.org/tools/framework-2.5.exe

2. Ejecutando el asistente de instalación

d:\dowonload\framework-2.5.exe

Instalando Metasploit Framework

Por citar un ejemplo, una de las principales diferencias entre Metasploit Framework y el resto de los productos mencionados, es el "foco". Mientras que los productos comerciales necesitan proveer constantemente a sus clientes los últimos exploits acompañados de interfaces gráficas cuidadas e intuitivas, el Framework de Metasploit se encuentra orientado principalmente a facilitar la investigación y experimentación con las nuevas tecnologías.
Aspectos como el mencionado hace que exista mercado para todos. Investigadores, estudiantes, curiosos e independientes, pueden obtener sin costo Metasploit, customizarlo hasta lograr que haga exactamente lo que uno desea, perfeccionarlo, o tan solo utilizarlo como plataforma de lanzamiento de Exploits en función de su trabajo, mientras que por su parte, grandes empresas que requieran de una excelente solución corporativa de sencilla utilización y puedan afrontar el costo, sin dudas se sentirán a gusto con la calidad, confiabilidad y servicios asociados de productos tales como Core Impact o Canvas.



Figura 1 Interfaz de Consola "MSFConsole", prompt interactivo.

Quién necesita de Metasploit Framework?

Hay muchas razones para obtener Metasploit Framework y ponerse a trabajar con el de inmediato. En primer lugar, aquellas personas interesadas en introducirse en el fabuloso mundo de programación de Exploits, encontraran en este framework, un excelente aliado puesto que su filosofía Open Source, hace que cada parte de código se encuentre disponible para quienes quieran matar su curiosidad y entender como funcionan las cosas.
En otro orden, si usted se encuentra trabajando como parte del staff de seguridad de una organización, probablemente deba permitirse desconfiar de los parches que su proveedor de software le ha suministrado para "solucionar" la ultima vulnerabilidad aparecida, y quiera intentar lanzar uno de los tantos Exploits de calidad incluidos en Metasploit sobre su propio sistema, a fin de evaluar si efectivamente el parche aplicado, ha corregido la vulnerabilidad informada o por el contrario sigue siendo posible explotarla.
Finalmente si su tarea es la de realizar puntualmente evaluaciones de seguridad... probablemente no necesite que desde estas páginas le recuerde la importancia de contar con un framework capaz de hacerle ahorrar varias horas de su valioso tiempo, permitiéndole además realizar test consistentes y repetibles, lanzar exploits de calidad comprobada, generar sus propias shellcodes y tantas otras cosas mas...
Recuerde que probablemente una de las mayores ventajas al momento de utilizar cualquiera de las herramientas mencionadas en el apartado anterior (Core Impact, Canvas y Metasploit), sea la posibilidad de contar con exploits probados, revisados y de alta calidad. Pero… por que es tan importante este punto? intentare ilustrar brevemente el concepto con un ejemplo... sucede que cada vez que una nueva vulnerabilidad es descubierta, comienzan a publicarse Exploits codificados por "entusiastas", los cuales a menudo no poseen la calidad necesaria a los efectos de realizar un trabajo profesional. Solo por dar un ejemplo, podría suceder que un exploit programado por principiantes, dada una vulnerabilidad x, logre explotar la misma, pero deje al sistema objetivo inestable o genere una denegación de servicio que requiera reiniciar el equipo atacado incluso cuando este no hubiera sido el objetivo inicial del testeo, mientras que por otra parte, un Exploit de calidad programado por expertos en dicho arte, probablemente se comporte en forma diferente, permitiéndole explotar la vulnerabilidad, tomar control remoto del equipo objetivo, y eventualmente abrir una puerta trasera a efectos de lograr persistencia y continuar con el proceso de "Penetration Testing" o "Ethical Hacking" sobre el cual se encuentra trabajando. Todo esto "de un solo disparo" (One Shot).
Por ultimo pero no por ello menos importante, si hay un motivo por el cual en mi opinión, usted debe conocer Metasploit Framework y lo que es capaz de hacer con el, es que los potenciales intrusos no solo ya lo conocen! sino que lo utilizan activamente!, de modo tal que el hecho de ignorar su potencialidad, sin dudas lo pondrá cuando menos en una situación de desventaja frente al atacante ocasional.

Interactuando con Metasploit Framework

Bien, puesto que no hay mejor forma de fijar conceptos, que poniendo manos a la obra, a través de los párrafos situados a continuación, me he propuesto guiarlo paso a paso a efectos de que pueda realizar su propia experiencia con esta magnifica herramienta.
Una vez instalado Metasploit Framework en su equipo (Ver "Instalando Metasploit Framework"), probablemente se encuentre ansioso por comprobar su funcionamiento.
En tal sentido y puesto que a fin de poner el Framework a trabajar, usted deberá interactuar con Metasploit, resultara imprescindible conocer que dicha interacción, podrá ser llevada a acabo por medio de la utilización de cualquiera de las siguientes interfaces:

Interfaz de Línea de Comando: Es la forma correcta de interactuar con el framework, cuando de automatizar secuencias de pruebas de exploits se trata, o sencillamente en aquellos casos que no se requiera una interfaz interactiva. La utilidad se ejecuta por medio del comando "msfcli".

Interfaz de Consola: Probablemente sea esta la interfaz comúnmente utilizada, debido a lo intuitivo de su uso interactivo, la rapidez de su operación y su flexibilidad. Su principal característica es la de brindarnos un "prompt" de Metasploit, a partir del cual podremos interactuar con cada uno de los aspectos del Framework. En caso de querer hacer uso de este modo, deberemos ejecutar el comando "msfconsole". Figura 1

Interfaz Web: Aunque posee muchos detractores, la interfaz web de metasploit puede ser de suma utilidad en ciertas circunstancias especiales, tal como presentaciones publicas o trabajo en equipo. A tal efecto, esta versión "web" de metasploit, incluye su propio servidor http, a fin de brindarnos la posibilidad de acceder vía browser a prácticamente las mismas características que en su versión de consola. Figuras 2

Exploits a la orden del día

Metasploit Framework, incluye como parte de su distribución, una serie de exploits listos para utilizar. A pesar de ello, existe una comunidad sumamente activa en torno a este producto, que periódicamente libera nuevos exploits, algunos de los cuales pueden ser adicionados fácilmente a nuestro Framework, por medio de una utilidad denominada "msfupdate", la cual a partir de la versión 2.2 es incluida como parte de la instalación estándar de Metasploit.

La actualización del framework es sumamente sencilla. Si usted ha instalado Metasploit en Windows, todo se reducirá a seleccionar en la carpeta correspondiente (Por defecto "Metasploit Framework") la utilidad de nombre "MSFUpdate". Si por el contrario su elección a pasado por GNU/Linux como plataforma de pruebas, bastara con ejecutar desde una consola, la utilidad "msfupdate":

```
fiona root # msfupdate -u
```

Una vez ejecutada, "msfupdate" nos mostrará información acerca de las ultimas novedades y pedirá nuestra confirmación a fin de hacer efectivo el update. Terminado el proceso, nuestro framework contará con los últimos exploits disponibles públicamente para Metasploit!!

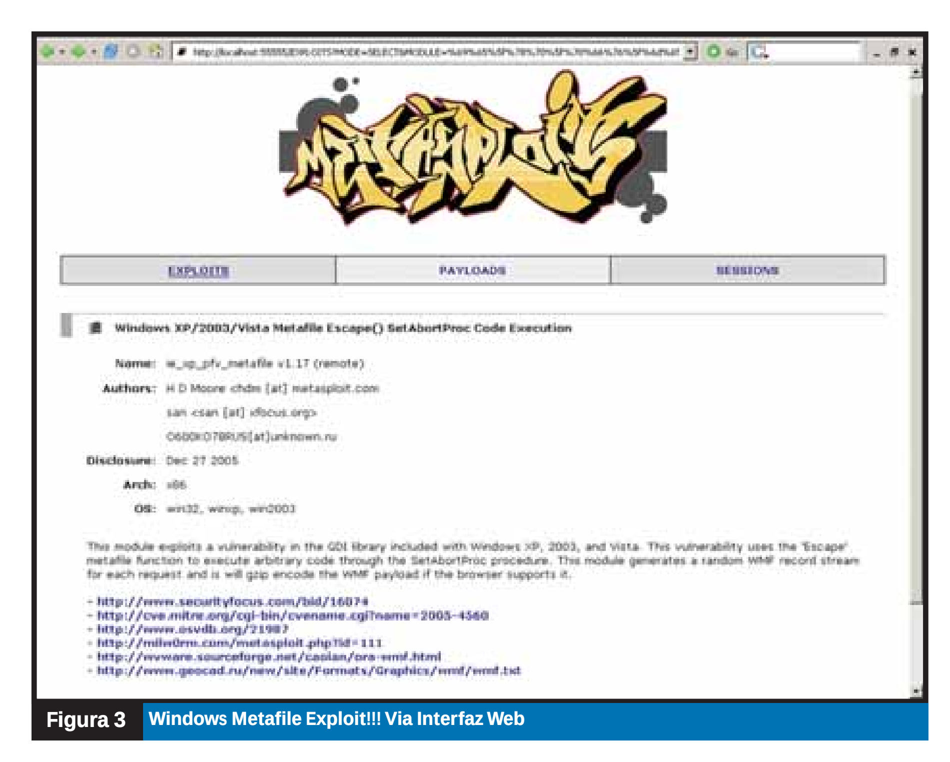


Figura 3 Windows Metafile Exploit!!! Via Interfaz Web

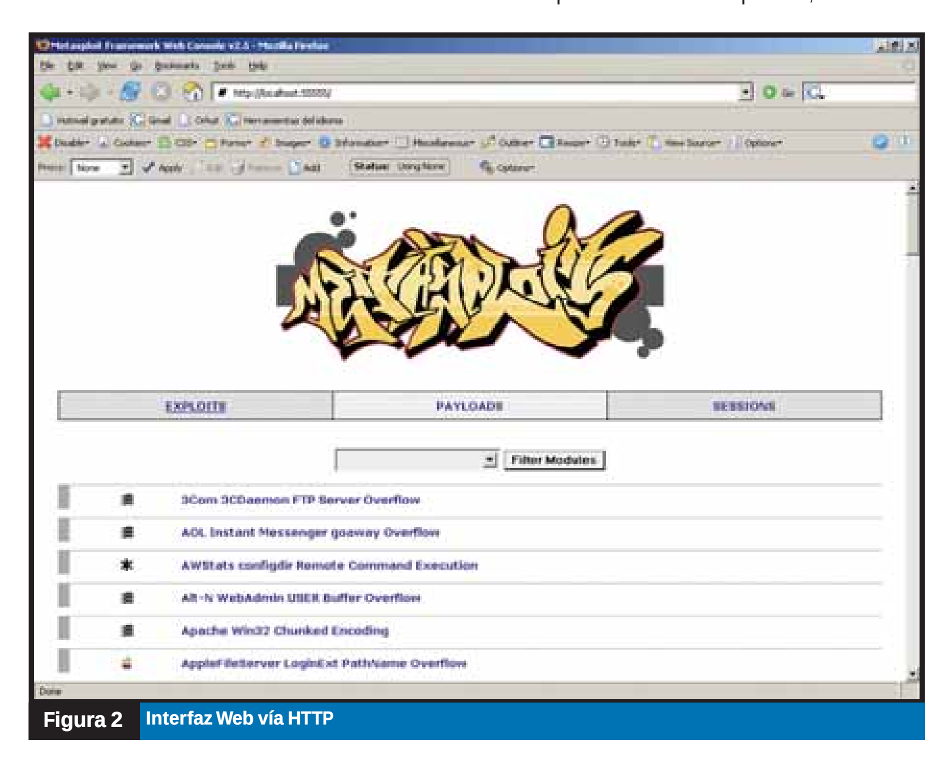


Figura 2 Interfaz Web vía HTTP

Tan solo un ejemplo

Llegado este punto, usted probablemente haya asimilado algunos nuevos conceptos, instalando la herramienta y procedido a actualizar su contenido, por lo tanto probablemente sea hora de comprobar si la instalación se ha realizado con éxito, y si Metasploit Framework realmente merece ocupar o no, un lugar privilegiado en su caja de herramientas.

Dicho esto y a modo de ejemplo, nos limitaremos en estas páginas a la utilización básica de la consola de Metasploit, de modo tal que esta pequeña practica, le permita luego aprovechar lo aprendido, a fin de seguir la misma metodología al momento de investigar todas y cada una de las variantes de las que nos provee este fantástico Framework.

En caso de que nuestra elección en cuanto a la plataforma de instalación de Metasploit haya pasado por GNU/Linux, deberemos acceder a la consola ejecutando:

```
fiona root # msfconsole
```

Si por el contrario hubiéramos decidido utilizar Windows, nuevamente bastara con seleccionar en la carpeta correspondiente (Nuevamente "Metasploit Framework") la utilidad de nombre "MSFConsole".

Luego de dar entrada o haber seleccionado este comando, según sea el caso, nuestra consola mostrara la pantalla de inicio de Metasploit ilustrada en la Figura 1, en la cual se podrá leer a su vez, información tal como la versión instalada, cantidad de Exploits y Payloads disponibles, y un prompt identificatorio (msf >) a partir del cual estaremos en condiciones de interactuar directa-

mente con el framework.
El set de comandos disponibles en Metasploit dependerá del contexto, o dicho de otro modo, el listado de los mismos podrá variar respecto de la sección del framework en la que nos encontremos. Por tal motivo, el primer comando que ejecutaremos una vez dentro del framework, será sin dudas el comando "help", el cual nos brindará una breve descripción de cada uno de los comandos y su efecto en el contexto actual.

msf > help

Lo primero que haremos, será echar un vistazo al listado de exploits disponibles, para lo cual deberemos ingresar el siguiente comando:

msf > show exploits

Como habrá podido observar, el listado de exploits es importante y mas que interesante (Ver "Algunos de los Exploits incluidos…"). A continuación seleccionaremos alguno que cumpla con las características necesarias para ser lanzado sobre nuestro equipo de pruebas (En mí caso un Windows 2000 Server SP 4), para lo cual deberemos echar mano al comando "use" pasando como parámetro el módulo de Exploit que hemos escogido para realizar nuestras pruebas:

msf > use lsass_ms04_011

Una instrucción de suma utilidad dentro de la consola de Metasploit, es aquella denominada "info". Aplicando este comando sobre alguno de los módulos del Framework, usted será capaz de obtener información adicional acerca del mismo. Por ejemplo en mi caso, en respuesta al comando:

msf lsass_ms04_011 > info lsass_ms04_01

He sido capaz de obtener datos tales como el de las versiones de Windows afectadas por la vulnerabilidad de la que se aprovecha este exploit, así como también una descripción general de su utilización, referencias a los boletines de seguridad publicados, nombre de el/los coder's, etc. (Figura 4)
Ok, llegado este punto ya hemos hecho nuestra elección respecto de un exploit apto para ser utilizado contra nuestra plataforma de pruebas, ahora deberemos decidir la "Shellcode" o "Payload" que metasploit ejecutará en caso de que la explotación pueda ser llevada a cabo. Otra vez, Metasploit nos brinda muchas posibilidades al respecto. Echemos un vistazo a los "Payloads" (Figura 5) disponibles para el exploit seleccionado:

msf lsass_ms04_011 > show payloads

En esta oportunidad probaremos suerte seleccionando "win32_bind" como el "Payload" a utilizar en este ejemplo. Si todo sale bien, y de acuerdo a las características de esta shellcode, una vez lanzado el exploit deberíamos poder acceder a una shell sobre el sistema remoto. Como hacemos para seleccionarlo? sencillo, deberemos asignar a la variable PAYLOAD, el valor adecuado mediante el comando "set", para lo cual deberemos introducir en la línea de comandos algo como:

msf lsass_ms04_011 > set PAYLOAD win32_bind

Recapitulemos… llegado este punto, hemos revisado la lista de exploits y payloads disponibles, obtenido mas información acerca de ellos y seteado nuestras preferencias (Exploit: lsass_ms04_01, Payload: win32_bind), ahora veamos las opciones que nos quedan por completar. Para dicha tarea tan solo tendremos que solicitar al Framework que nos muestre las opciones disponibles para el entorno seleccionado:

msf lsass_ms04_011 (win32_bind) > show options

La ejecución de este ultimo comando, nos

Figura 4 Utilizando el comando "info" para conocer algo más acerca de un exploit

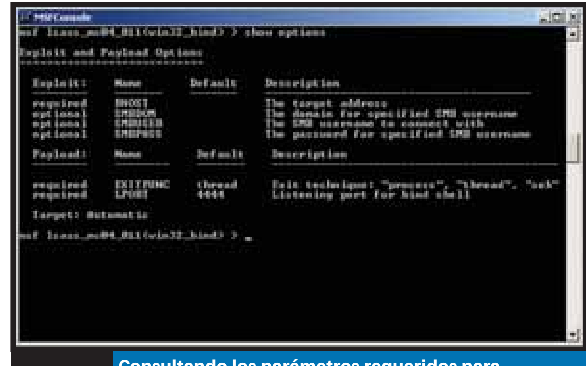


Figura 5 Algunos de los Payloads Incluidos en Metasploit FW

Figura 6 Consultando los parámetros requeridos para el exploit seleccionado

En Beta: Ruby... Todo lo que brilla es Oro!!

Hace tan solo algunas semanas, la gente del proyecto Metasploit publicaba en su sitio oficial la disponibilidad de la versión Beta 3.0 de su framework. A diferencia de los upgrades anteriores, la futura versión 3.0 de Metasploit Framework incluirá una serie de cambios esperados e importantes, tanto que los mismos incluso habrían motivado el salto de familia!! (esto es 3.x en vez de 2.x).
Respecto de su predecesor 2.5, sin dudas uno de los aspectos más llamativos, haya sido el cambio de lenguaje de programación utilizado para soportar el framework. El grupo de desarrollo, luego de varias semanas de debate, ha decidido echar manos a "Ruby" un lenguaje de programación interpretado y orientado a objetos muy especial, el cual vendría a reemplazar la utilización del viejo código escrito en Perl.
Por lo que se puede observar de la beta publicada, la capacidad de "Ruby" a permitido crear un código mas compacto y ágil, el cual seguro será aprovechado por la comunidad para dotar de nuevos componentes esta magnifica versión que planea revolucionar la forma en la que las tareas relacionadas con el framework son llevadas a cabo.
Por su parte, las capacidades de meterpreter han sido mejoradas definitivamente, permitiendo realizar algunas pocas acciones que hasta este momento solo era posible realizar con alguna otra herramienta comercial.
Si bien es cierto que de momento, esta beta solo se encuentra disponible para ser ejecutada en entornos Unix/Linux, es de esperar que la versión final soporte otras plataformas. De este modo, si tiene ganas de colaborar con el proyecto, solo deberá descargar esta nueva versión, realizar sus propias pruebas y postear sus comentarios! Seguramente serán tenidos en cuenta y colaboraran a que todos disfrutemos en algunas semanas, de una herramienta sumamente mejorada.

permite conocer las variables/opciones disponibles a la hora de configurar la dupla exploit/payload que estamos a punto de ejecutar (Figura 6). En muchos casos, alguna de las opciones requeridas se completara con valores por defecto en forma automática, aunque siempre habrá que setear por ejemplo, aspectos tales como la dirección IP de nuestro TARGET (RHOST). Del mismo modo podríamos si quisiéramos cambiar el puerto de escucha propuesto por defecto por el framework (LPORT). El comando que debemos utilizar al momento de asignar valores a estas variables es "set". Puesto que en mi entorno de pruebas, el target se encuentra tras la IP 172.16.1.96, el conjunto de comandos ingresados en mi consola lucirá del siguiente modo:

```
msf lsass_ms04_011 (win32_bind) > set RHOST 172.16.1.96
msf lsass_ms04_011 (win32_bind) > show options
```

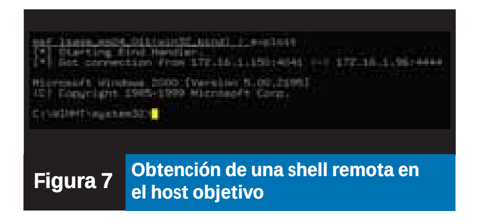
Con el primero he definido el host destino, y con el segundo verificaré que no me haya olvidando de suministrar algún parámetro antes de lanzar mi exploit!!!
Ok, habiendo corroborado la información suministrada al Framework hasta aquí, tan solo deberemos ejecutar el Exploit seleccionado y ver que sucede, para lo cual enviaremos precisamente, el comando de nombre "Exploit" para que el mismo se ejecutado:

```
msf lsass_ms04_011 (win32_bind) > exploit
```

En hora buena, si todo ha salido tal lo planeado, como puede observar en la Figura 7, tan solo unos segundos después de lanzado el exploit, hemos obtenido un fantástico shell, el cual según lo informado por Metasploit, se encuentra linkeado a través del port 4444. Objetivo cumplido, sencillo no es cierto?.

Conclusión

A lo largo del presente artículo, hemos sido capaces de observar la sencillez con que algunas acciones pueden ser llevadas a cabo, por medio de la utilización de Metasploit Framework. A pesar de ello, demás esta decir que lo mostrado es tan solo uno de los tantos usos que pueden hacerse del mismo.
Como mencionara al introducir el articulo, la intención no era mas que la de tan solo presentar la herramienta a aquellas personas que aun no habían tenido la oportunidad de conocerla, de modo tal de despertar su curiosidad e invitarlo a investigar por usted mismo las muchas formas en la que Metasploit Framework puede colaborar con la tarea diaria de su departamento interno de seguridad.
Hoy en día, muchas empresas han establecido rutinas de trabajo específicas durante las cuales se ejecuta alguna herramienta automatizada de búsqueda de vulnerabilidades. En dicho escenario, Metasploit Framework podría representar un excelente complemento cuando de chequear falsos positivos se trata, el hecho que mediante su utilización, usted tenga la posibilidad de ser capaz de explotar realmente la vulnerabilidad reportada por las herramientas utilizadas en su organización, le permitirá obtener un punto de vista distinto del grado de criticidad señalado por dichas herramientas.
De todos modos y siendo recurrentes, Metasploit Framework es mucho más que una interfase para lanzar exploits. Cada uno de los módulos incluidos en el framework, se encuentran a su disposición!!. De esta forma para los mas avanzados, el desarrollo de sus propios exploits haciendo uso de librerías y rutinas estándar, le proporcionara una plataforma esencial a la hora de ganar tiempo re-utilizando shellcodes y objetos de uso común, al tiempo que le permitirá aprender de la lectura del código fuente.
De más esta decir que la utilización de Metasploit, debe ser considerada una herramienta más al alcance del profesional. Bajo ningún punto de vista, el uso de esta o cualquier otra herramienta reemplazara la necesidad de contar con un staff de seguridad altamente capacitado o la pericia de recursos especializados en practicas de intrusión controladas, quienes a menudo encontraran el modo de brindar valor agregado a la utilización de esta u otras herramientas, en pro de la solución de negocios propuesta, basados en técnica, inventiva, experiencia y acción metodologica.
Hecha la aclaración de rigor y resumiendo, Metasploit Framework es una excelente herramienta mas con la cual usted podrá contar, al momento de evaluar la seguridad de sus sistemas. Open Source, gratuita, de libre distribución y con una comunidad sumamente activa que no pierde pisada a la aparición de nuevas vulnerabilidades, esta sin dudas se convertirá rápidamente en una de sus preferidas. No obstante ello, sin dudas los mas curiosos encontraran en el Framework horas de sana diversión, experimentando con aspectos tal como meterpreter u otras tantas características avanzadas que han logrado hacer de esta, una herramienta imprescindible. ■


Figura 7 Obtención de una shell remota en el host objetivo

apache_chunked_win32	Apache Win32 Chunked Encoding
cabrightstor_disco	CA BrightStor Discovery Service Overflow
exchange2000_xexch50	Exchange 2000 MS03-46 Heap Overflow
freeftpd_user	freeFTPd USER Overflow
ie_xp_pfv_metafile	**Windows XP/2003/Vista Metafile Escape() SetAbortProc Code Execution**
iis40_htr	IIS 4.0 .HTR Buffer Overflow
iis50_printer_overflow	IIS 5.0 Printer Buffer Overflow
iis50_webdav_ntdll	IIS 5.0 WebDAV ntdll.dll Overflow
iis_fp30reg_chunked	IIS FrontPage fp30reg.dll Chunked Overflow
iis_nsiislog_post	IIS nsiislog.dll ISAPI POST Overflow
iis_source_dumper	IIS Web Application Source Code Disclosure
iis_w3who_overflow	IIS w3who.dll ISAPI Overflow
imail_imap_delete	IMail IMAP4D Delete Overflow
imail_ldap	IMail LDAP Service Buffer Overflow
irix_lpsched_exec	IRIX lpsched Command Execution
lsass_ms04_011	Microsoft LSASS MS04-011 Overflow () Code Execution
ms05_039_pnp	Microsoft PnP MS05-039 Overflow
msasn1_ms04_007_killbill	Microsoft ASN.1 Library Bitstring Heap Overflow
msmq_deleteobject_ms05_017	Microsoft Message Queueing Service MS05-017
msrpc_dcom_ms03_026	Microsoft RPC DCOM MS03-026
mssql2000_preauthentication	MSSQL 2000/MSDE Hello Buffer Overflow
mssql2000_resolution	MSSQL 2000/MSDE Resolution Overflow
oracle9i_xdb_ftp	Oracle 9i XDB FTP UNLOCK Overflow (win32)
oracle9i_xdb_ftp_pass	Oracle 9i XDB FTP PASS Overflow (win32)
oracle9i_xdb_http	Oracle 9i XDB HTTP PASS Overflow (win32)
samba_nttrans	Samba Fragment Reassembly Overflow
sambar6_search_results	Sambar 6 Search Results Buffer Overflow
solaris_dtspcd_noir	Solaris dtspcd Heap Overflow
solaris_kcms_readfile	Solaris KCMS Arbitary File Read
solaris_lpd_exec	Solaris LPD Command Execution
warftpd_165_pass	War-FTPD 1.65 PASS Overflow
warftpd_165_user	War-FTPD 1.65 USER Overflow
windows_ssl_pct	Microsoft SSL PCT MS04-011 Overflow
wins_ms04_045	Microsoft WINS MS04-045 Code Execution
wsftp_server_503_mkd	WS-FTP Server 5.03 MKD Overflow

Algunos de los Exploits incluidos en Metasploit Framework

Referencias y Lectura Complementaria

Sitio Oficial del Proyecto Metasploit
http://www.metasploit.org

Sitio Oficial de Ruby
http://www.ruby.org

Sitio Oficial del Producto Canvas
http://www.immunitysec.com/products-canvas.shtml

Sitio Oficial del Producto Core Impact
http://www.coresecurity.com/products/coreimpact/index.php

Mi Distribución de Linux Preferida
http://www.gentoo.org

Presentaciones varias respecto de ISECOM, OSSTMM y prácticas de testeo y seguridad
http://www.hernanracciatti.com.ar
http://www.sicinformatica.com.ar



BASES DE DATOS
Historia y Conceptos Básicos

Alejandro Cynowicz
Editor Técnico - Revista NEX IT Specialist

Hoy las empresas no podrían concebir su modelo de negocios sin esta herramienta clave para organizar sus finanzas y la atención de sus clientes. Veremos la evolución de las bases de datos y cómo fue vinculándose fuertemente con el sector IT.

En este artículo presentaremos los conceptos básicos de base de datos (en particular de los sistemas gestores que manejan los datos de la base) a través de su historia y conociendo a la gente que desarrolló los conceptos fundamentales. NEX IT Specialist contribuye con parte de este artículo a Wikipedia (http://es.wikipedia.org/wiki/Sistema_de_gestión_de_base_de_datos)

Empezaremos por definir que es una Base de Datos, y distinguiremos a las aplicaciones de base de datos, del Sistema Gestor De Base De Datos:
- Base de datos: es un conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su uso posterior. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.

- Aplicación de base de datos: es un software de computadora escrito para organizar los datos de una aplicación en particular o problema.

- Sistema Gestor De Base De Datos (SGBD) es un programa de computadora (o más frecuentemente una suite de software) diseñado para manejar una base de datos (un gran conjunto de datos estructurados) y corre operaciones en los datos requeridos por numerosos clientes. Los SGBD son encontrados en el corazón de la mayoría de las aplicaciones de bases de datos. Algunas veces los SGBD son construidos alrededor de un kernel multitarea privado con soporte para networking incorporado, aunque hoy en día estas funciones son dejadas al sistema operativo. Podemos encontrar ejemplos de usos típicos de SGBD en contabilidad, recursos humanos y sistemas de atención al cliente. Originalmente sólo se los hallaba en organizaciones con el hardware necesario para soportar enormes conjuntos de datos; recientemente los SGBD han emergido como una herramienta estándar en las oficinas de cualquier compañía.

Historia
Las bases de datos han estado en uso desde los comienzos de la computación electrónica, pero la vasta mayoría de éstas eran programas personalizados (hechos a medida) escritos para acceder bases de datos creadas especialmente para estos programas. A diferencia de los sistemas modernos que pueden aplicarse a una amplia variedad de bases de datos y necesidades, estos sistemas estaban rígidamente vinculados a su propia base de datos para aumentar su velocidad a cambio de flexibilidad.



POR FIN, EL E-MAIL VOLVERÁ A SER UNICAMENTE E-MAIL.

Volvamos a aquellos días en que su e-mail no se confabulaba con virus, gusanos, spam, spam y más spam. Con las soluciones E-mail Security de Symantec, la cantidad de e-mail no deseado que satura las bandejas de entrada de su organización puede ser drásticamente reducida. Con la combinación de más de 20 tecnologías de filtros-spam con el líder en antivirus, las soluciones Symantec E-mail Security erradican el spam, destruyen los virus y bloquean contenidos indeseables y peligrosos. Y con menos desorden en sus e-mails, la gente será más productiva, los tiempos muertos serán menores y al final, su infraestructura se volverá más flexible y resistente. ¿Extraña los e-mails como eran antes? Es tiempo de recuperarlos. Visite www.symantec.com/offer y utilize el código 14132 para obtener mayor información. **BE FEARLESS.**

symantec.

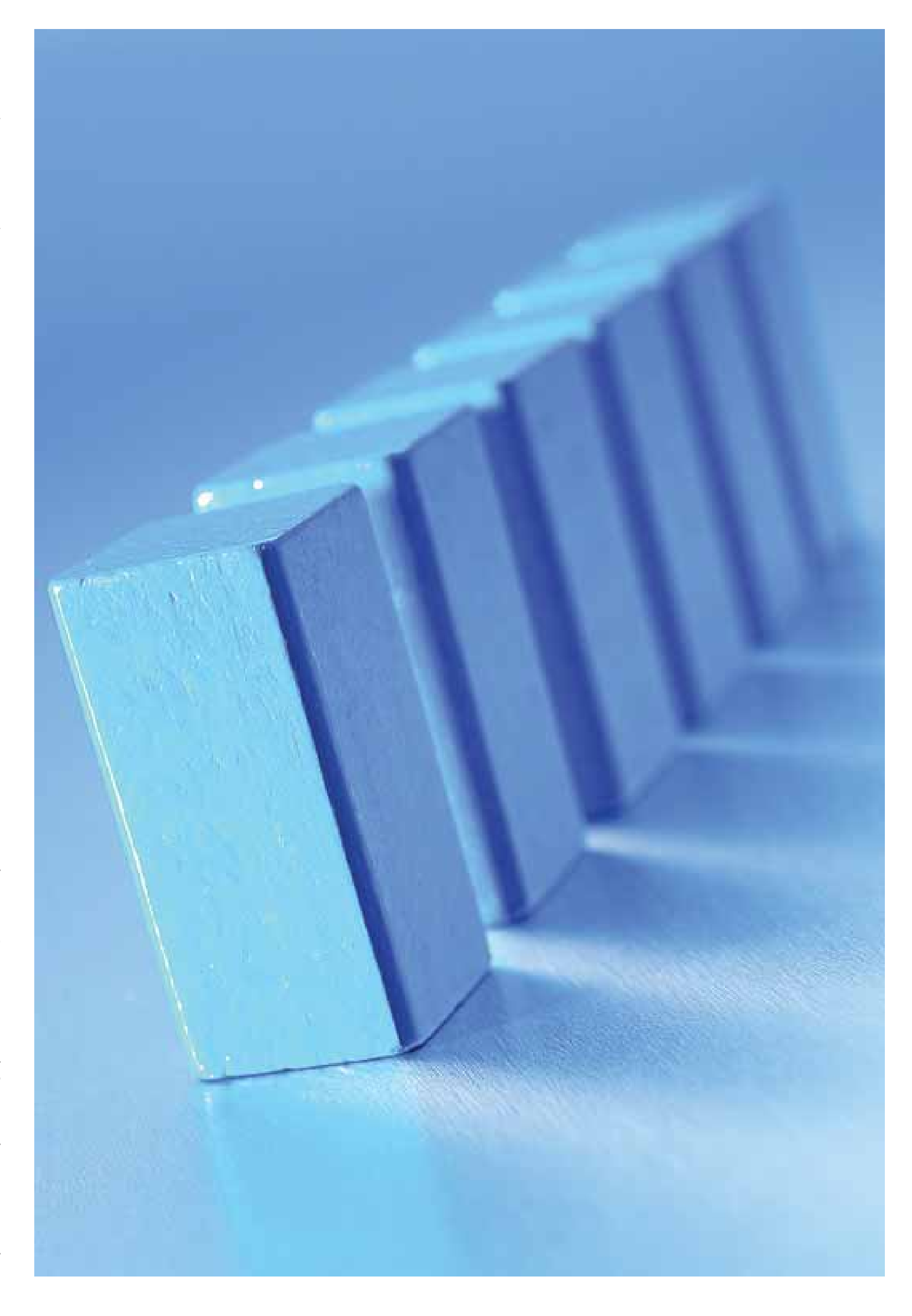
SGBD Navegable

A medida que las computadoras crecían en capacidad, el sacrificio de compatibilidad a cambio de performance se volvió cada vez más innecesario y emergieron algunas bases de datos para usos generales; hacia mediados de los '60 había un número de estos sistemas en uso comercial. Comenzó a crecer el interés en un estándar, y Charles Bachman, autor de uno de aquellos productos, IDS, fundó el Database Task Group dentro de CODASYL, el grupo responsable de la creación y estandarización del COBOL. En 1971 ellos lanzaron su estándar, que en general se volvió conocido como el Approach CODASYL (método o enfoque CODASYL), y pronto había disponibles varios productos comerciales basados en éste.

Él enfoque CODASYL estaba basado en la navegación "manual" de un conjunto de datos linkeado, que conformaba una red mayor. Cuando la base de datos era abierta por primera vez, al programa se le enviaba un link al primer registro de la base de datos, el cual también contenía punteros a otros datos. Para encontrar algún registro en particular, el programador tenía que pararse en cada uno de los punteros, uno a la vez hasta que el registro requerido fuese hallado. Simples búsquedas como "encontrar toda la gente en Suecia" requería que el programa caminara por el conjunto de datos entero y recoger los resultados coincidentes. Esencialmente, no había un concepto de "buscar". Ésto debe sonarnos como una limitación muy seria hoy, pero en una era en la que usualmente los datos eran almacenados en su mayoría en cintas magnéticas, tales operaciones eran de cualquier manera muy caras como para contemplarlas.

IBM también tuvo su propio sistema SGBD en 1968, conocido como ISM. Éste era un desarrollo de software escrito para el programa Apollo (de la N.A.S.A.) en el sistema System/360. IMS era similar en concepto a CODASYL, pero para su modelo de navegación usaba un sistema de jerarquía estricta en lugar del modelo de red del CODASYL.

Ambos conceptos luego fueron conocidos como bases de datos navegables debido a la forma en que los datos eran accedidos, y porque cuando a Bachean se le otorgó el premio Turing en 1973, su presentación se tituló "The Programmer As Navigator" (El Programador Como Navegante). IMS está clasificado como una base de datos jerárquica. IDS y IDMS (ambos son bases de datos CODASYL) y la CINCOMs TOTAL, son clasificadas como bases de datos de redes (Network Databases).



SGBD Relacional

Edgar Codd trabajó en IBM en San José, California, en una de sus oficinas de proyectos especiales que estaba principalmente involucrada en el desarrollo de sistemas de discos rígidos. Él estaba insatisfecho con el sistema navegable del método CODASYL, en especial la falta de la función de búsqueda, la que estaba convirtiéndose en cada vez más útil cuando la base de datos era almacenada en un disco en lugar de una cinta.

En 1970, Codd escribió unos trabajos científicos que delinearon un nuevo enfoque en la construcción de bases de datos que eventualmente culminaría en el revolucionario "Un Modelo Relacional de Datos para grandes bancos de datos compartidos." (A Relational Model of Data for Large Shared Data Banks).

En este ensayo describió un nuevo sistema para almacenar y trabajar con grandes bases de datos. En lugar de guardar los registros en algún tipo de lista vinculada de registros en forma libre como en CODASYL, la idea de Codd era usar una tabla de registros de longitud fija. Un sistema de lista linkeada sería muy ineficiente para almacenar base de datos "Sparse" donde algunos de los datos para cualquiera de los registros serían dejados vacíos. El modelo relacional resolvió esto dividendo los datos en series de tablas, con elementos opcionales siendo movidos afuera de la tabla principal hacia donde ocuparían lugar sólo si son necesitados.

Por ejemplo, un uso común de un sistema de base de datos es para rastrear información acerca de usuarios, sus nombres, información de login, varios domicilios y números de teléfonos. En el método relacional, los datos serían divididos en una tabla de usuarios, una de domicilios y una tabla de teléfonos (por ejemplo). Los registros serían creados en esas tablas opcionales sólo si el domicilio o el número de teléfono fueron ingresados.

Vincular la información consigo misma es la clave de éste sistema. En el modelo relacional algunas pequeñas partes de información eran usadas como una "llave" (key), definiendo un registro en particular de forma única. Cuando la información acerca de un usuario era recolectada, los datos almacenados en la tabla opcional (o relacionada) serían encontrados buscando esta llave. Por ejem-

plo, si el nombre de login de un usuario es único, los domicilios y números telefónicos para ese usuario serían registrados con el nombre de login como su clave. Esta "re-vinculación" de datos relacionados en una sola colección es algo para lo que los lenguajes de programación tradicionales no están diseñados (fig. 1)

Así como el método navegable requeriría de ciclos repetitivos para recolectar información acerca de cualquier registro, el enfoque relacional requeriría loops (ciclos repetitivos) para recolectar la información de un registro dado. La solución de Codd para los dichos ciclos necesarios fue un lenguaje orientado al conjunto (set oriented), una sugerencia que luego devendría en el conocido SQL.

Usando una rama de las matemáticas conocida como cálculo tuple, demostró que tal sistema podría soportar todas las operaciones de base de datos normales (insertar, actualizar, etc.) así como proveer un sistema simple para hallar y entregar conjuntos de datos en una sola operación.

El trabajo científico de Codd, fue usado por dos personas en Berkeley, Eugene Wong y Michael Stonebraker. Ellos comenzaron un proyecto conocido como INGRES usando fondos que ya habían sido previamente otorgados para un proyecto de base de datos geográfica, usando estudiantes de programación para producir código. Comenzando en 1973, INGRES produjo sus primeros productos de prueba, los que estuvieron en términos generales listos para su uso extendido en 1979. Durante este tiempo algunas personas se habían

"key"

login	first	last
mark	Samuel	Clemens
lion	Lion	Kimbro
kitty	Amber	Straub

login	phone
mark	555.555.5555

"related table"

Figura 1 Claves relacionales

movido dentro del grupo, quizás hasta 30 personas llegaron a trabajar en el proyecto, alrededor de 5 a la misma vez. INGRES era similar a System R en varias maneras, incluyendo el uso de un lenguaje para acceder a los datos, conocido como QUEL; éste era de hecho relacional, ya que estaba basado en el lenguaje Alpha escrito por Codd, pero desde entonces ha sido modificado para seguir al SQL, violando tantos conceptos del modelo relacional como el mismo SQL.

IBM hizo sólo un test de implementación del modelo relacional, PRTV, y uno de producción, Business System 12, ambos discontinuados al día de hoy. Honeywell hizo el MRDS para Multics, y ahora hay dos nuevas implementaciones: Alphora Dataphor y Rel. Todas las otras implementaciones de SGBD usualmente llamadas relacionales son de hecho SQL SGBDs.

SQL SGBD

IBM comenzó a trabajar en un sistema prototipo basado a medias en conceptos de Codd, como el System R a comienzos de los '70s. Desafortunadamente, System R fue concebido como una forma de probar que las ideas de Codd no eran implementables y por consiguiente el proyecto le fue entregado a un grupo de programadores quienes no estaban bajo la supervisión de Codd y nunca entendieron sus ideas por completo y terminaron violando muchos fundamentos del modelo relacional. La primera versión "rapidita" estuvo lista en 1974/5, y entonces comenzó el trabajo en sistemas multi-tablas en los cuales los datos podrías ser divididos para que todos los datos en un registro (muchos de los cuales son opcionales) no tuvieran que ser almacenados en un solo y largo "chorro". Subsecuentemente, versiones multi-usuario fueron testeadas por consumidores en 1978 y '79, para entonces un lenguaje estandarizado, el SQL, había sido agregado. Las ideas de Codd se estaban estableciendo como trabajables y superiores a CODASYL, presionando a IBM a desarrollar una verdadera versión de producción del System R, conocida como SQL/DS, y luego, Database 2 (DB 2).

Varios de los involucrados con INGRES se convencieron del futuro éxito comercial de tal sistema, y formaron su propia compañía para comercializar el trabajo pero con una interfaz SQL. Sybase, Informix, NonStop SQL y eventualmente INGRES misma fueron todas vendidas como derivados del producto INGRES original en los '80s. Aun el Microsoft SQL Server es de hecho una versión reconstruida de Sybase, y por lo tanto INGRES. Sólo Oracle (de Larry Ellison) comenzó desde una línea diferente, basándose en trabajos científicos de IBM sobre System R, logrando salir al mercado antes al presentar su versión en 1978.

Stonebraker aplicó la lección de INGRES para desarrollar una nueva base de datos, Postgres, hoy conocida como PostgreSQL y es ahora una de las bases de datos más ampliamente usadas en el mundo, principalmente para aplicaciones globales de misiones críticas (los registros de dominios .org y .info la usan como almacenamiento primario de sus datos, al igual que muchas grandes compañías e instituciones financieras).

En Suecia, el trabajo científico de Codd fue leído también, Mimer SQL fue desarrollado a mediados de los '70 en la universidad de Uppsala, y en 1984 este proyecto fue consolidado en una empresa independiente. A comienzos de 1980 Mimer introdujo el manejo de transacciones para alta robustez en aplicaciones, una idea que fue subsecuentemente implementada en la mayoría de las SGBDs

SGBD Orientado a Objetos:

SGBD Multidimensional tuvo un impacto duradero en el mercado: condujeron directamente al desarrollo de sistemas de bases de datos de objetos. Basadas en la misma estructura general y conceptos que el sistema multidimensional, esos nuevos sistemas permitieron al usuario almacenar objetos directamente en la base de datos en lugar de primero convertirla en algún otro formato.

Ésto fue posible gracias al concepto de "ownership" (propietario) del sistema multidimensional. En un programa orientado a objetos (OO), un objeto particular típicamente contendrá otros; por ejemplo, el objeto representando a Bob pude contener una referencia a un objeto separado que hace referencia al domicilio de Bob. Agregando soporte para varios lenguajes OO y polimorfismo, recrea el sistema multidimensional como objeto de base de datos, lo que le permite atender a un nicho hasta el día de hoy. ■

Las Certificaciones más importantes del 2005

En NEX #21 publicamos un ranking de certificaciones internacionales basadas básicamente en el criterio de crecimiento, reputación y aceptación elaborado por certcities.com.

CertCities ha publicado muy recientemente otro ranking. Su Annual "Readers Choise Awards" indicando las certificaciones top elegidas por sus lectores: *http://certcities.com/editorial/features/story.asp?EditorialsID=94*

En este caso los ganadores están seleccionados por profesionales IT (no periodistas o vendors en certificaciones). De algún modo obtenemos un criterio diferente e interesante sobre qué certificaciones son las más buscadas o populares en 2006 y por ende tienen valor en el mundo "real".

Networking y seguridad continúan siendo tópicos muy importantes y la selección por parte de los profesionales IT son particularmente destacables. Si uno está planificando el futuro de una carrera en IT éstas deberán estar incluidas (o consideradas).



Mejor nivel Certificación Entry-Level (nivel inicial).	*Ganadora:* CompTIA A+ *Finalistas:* Microsoft Certified Professional (MCP) & Cisco Certified Network Associate (CCNA)
Mejor Certificación Mid-Level de Networking (nivel medio)	*Ganadora:* **Microsoft Certified Systems Administrator (MCSA)** *Finalistas:* Cisco Certified Network Professional (CCNP) & CompTIA Server+
Certificación High Level (Nivel Alto) más resepetada.	*Ganadora:* **Cisco Certified Internetwork Expert (CCIE)** *Finalistas:* Microsoft Certified Systems Engineer (MCSE) & (ISC)2 Certified Information Systems Security Professional (CISSP)
Mejor Certificación de Seguridad.	*Ganadora:* **(ISC)2 CISSP** *Finalistas:* Cisco Certified Security Professional (CCSP) & Microsoft Certified Systems Engineer: Security (MCSE: Security)
Mejor Certificación de desarrollo.	*Ganadora:* **Microsoft Certified Solutions Developer (MCSD)** *Finalistas:* Oracle Forms Developer, Sun Certified Java Developer (SCJD)
Mejor Certificación de Bases de Datos.	*Ganadora:* **Microsoft Certified Solutions Developer (MCSD)** *Finalistas:* Oracle Forms Developer, Sun Certified Java Developer (SCJD)
Mejor Certificación de Internet.	*Ganadora:* **Adobe Dreamweaver Developer** *Finalistas:* Prosoft Certified Internet Webmaster (CIW) Professional, CompTIA i-Net+
Mejor Certificación Linux/Unix.	*Ganadora:* **Red Hat Certified Engineer (RHCE)** *Finalistas:* Sun Certified Systems Administrator, Solaris (SCSA Solaris), CompTIA Linux+

Más Ganadores de interés a las certificaciones

Mejores Guias de estudio para certificaciones
Ganador: Microsoft Press
Finalistas: Que Exam Cram 2, Sybex

Mejores Exámenes de practica
Ganador: Transcender
Finalistas: Self Test, MeasureUp

Autor Favorito de Guias de estudio
Ganador: Mike Meyers
Finalistas: Todd Lammle, Ed Tittel, Shon Harris

Autor Tecnico Favorito
Ganador: Mark Minasi
Finalistas: Mark Russinovich, Don Jones, Todd Redmond



Mejor Programa de Certificación

CISCO SYSTEMS

Qué nos dice Dan Hong de Cercities de esta categoría tan importante "…El programa de Cisco continúa por cuarto año consecutivo ganándole a competidores como Microsoft y CompTIA..."
Aparentemente, a los profesionales de IT les encanta el dolor y respetan las dificultades que CISCO pone en sus exámenes de certificación. Pero, la dificultad de los exámes es proporcional al respecto y reconocimiento de los "pares" (peers) y empleadores.
Veamos que dicen algunos de los lectores del porque de CISCO como elección:

" Cisco ha mantenido siempre sus certificaciones al día y resistentes a las llamadas "paper certifications"."

"Los examenes CISCO son bastante dificiles y requieren altos percentajes para aprobar y tienen más preguntas con simulaciones. Creo que las certificaciones CISCO son muy precisas en medir el grado técnico de quien rinde".

Microsoft









(IN)SATISFACCIÓN LABORAL del profesional IT

Maximiliano S. Di Toro
Network Administrator

"Windows IT Pro", es una de las revistas más prestigiosa del mundo de profesionales de IT (www.windowsitpro.com). Es un medio independiente y especializado en tecnologías Microsoft. En su edición de Diciembre de 2005, y como lo hace año a año publicó un estudio sobre sueldos y satisfacción con el trabajo en IT. Windows IT Pro realizó su "IT Industry Survey 2005" durante casi un mes, enviando invitaciones a 70.000 profesionales. Un total de 1728 respondieron al estudio que constaba de 61 preguntas.

Los resultados de las encuestas de Windows IT Pro me resultaron de algún modo predecibles, me sentí reflejado en muchas de las respuestas dadas en su estudio. Aunque no se crea, también ayudó, a concientizar a mi jefe del aumento que estaba yo necesitando.

Salario	%
$200.000 o más	0.5%
$150.000 a 199.999	1%
$125.000 a 149.999	2%
$100.000 a 124.999	7%
$90.000 a 99.999	6%
$80.000 a 89.999	10%
$70.000 a 79.000	13%
$60.000 a 69.999	16%
$50.000 a 59.999	16%
$40.000 a 49.999	12%
$30.000 a 39.999	8%
Debajo de $30.000	7%

...Y no, no es éste el grafico en el cuál me siento reflejado.

Veamos entonces algunas de las conclusiones

Uno de los resultados que más me asombró fue que el 11% de los trabajadores IT son "Trabajadoras "si señores "ellas" están aquí y cada vez son más; señoras y señoritas Bienvenidas.

Los sueldos no fueron tan distintos a lo que me imaginaba que se manejaban en el Norte del continente. (Estados Unidos y Canadá)

Otro dato interesante es que el 40% no tiene ningún tipo de certificación, mientras que dentro del 60% con certificaciones, las más populares son MCSA, MCSE y MCP.

Algo que llamó mi atención es que, mientras un 14.6% de los profesionales IT que poseen algún tipo de certificación Microsoft pueden alcanzar un salario de más de U$S 100.000, el 17.5% de los profesionales IT sin certificación pueden aspirar a la misma suma. La diferencia entre poseer o no una certificación, sólo la podemos encontrar en los sueldos comprendidos en el rango entre U$S 60.000 y U$S 99.999, en donde el número de profesionales con certificaciones superan a los que no las poseen (49.3% contra el 43%).

Y ¿que arrojó el estudio respecto a la satisfacción laboral?

Una gran parte de la insatisfacción proviene de la presión puesta sobre los IT Pros para cumplir con las necesidades de los empleadores de obtener soluciones IT que funcionen, que no tengan un alto costo de adquisición y mantenimiento, y no requieran una administración muy compleja. También hay otros factores influyentes en la satisfacción laboral, como la cantidad de horas trabajadas.

Por supuesto uno de los factores con mayor influencia en la satisfacción laboral es la **compensación**. Pero, curiosamente, el 50% de quienes respondieron piensan que están compensados en remuneración adecuadamente. Es decir el factor salario no es el único importante a la hora de valorar la satisfacción. Mucho tiene que ver con la razón de porqué un IT Pro tiene este trabajo: Tecnología y los desafíos de trabajar con ella.

¿Entonces, de entre los 19 tópicos que se censaron bajo la consigna: "Problemas en el Trabajo que causan mayor stress": ¿Cuál rankeó #1?

Respuesta: Insuficiente personal para poder lograr la tarea en tiempo y forma.

Terminando la nota se concluye que cada uno de los profesionales tiene una manera particular de responder al interrogante principal planteado por el artículo: ¿Estás contento con tu sueldo?

Lo que queda claro es que sin importar en dónde trabaja, varón o mujer, si lo hace en el ambiente IT va a tener un trabajo duro, bastante bien remunerado, estable (casi 70% lleva más de 10 años en el mismo empleo), cuanto más Senior mejor recompensado, y en el que muchas de las tareas más estresantes que hará no tendrán que ver estrictamente con la tecnología. Quizás lo que queda por preguntar es, en todo caso ¿Cómo Usted solucionaría las insatisfacciones que le genera su trabajo? Después de redactar esta nota me quedé pensando (no sólo en los sueldos con un promedio anual de U$S 67.878!!! (algo como $ 17.000 pesos por mes)) ¿Qué arrojaría un estudio similar sobre la situación en Argentina de los trabajadores IT? A tal fin propuse al director de NEX realizar tal estudio. Esperamos poder concretarlo (dependerá de vuestra colaboración) y presentar a nuestros lectores los resultados en marzo de este año 2006. ■

Nota 1

Cuando el director de la revista, me propuso escribir esta serie de notas, debo confesar que me sentí un poco perturbado. No es poca la tarea de condensar un planteo integral de seguridad, desde sus bases, y de manera que resulte entendible, en poco espacio. Por lo menos, no para mí. Pero al final, después de darle no pocas vueltas, la idea se fue plasmando en esas letras que ahora les llegan.

Estructuré estas notas de manera modular, es decir, no es necesario leer la serie entera. Cada una abordará un escalón de un planteo de seguridad, desde lo más básico, la instalación -motivo de este primer artículo- hasta la seguridad en una red, sea esta grande o pequeña, con la que finalizaremos.

Trataré de ceñirme a los lineamientos generales de Linux, sin hacer foco en ninguna distribución, y evitando hacer hincapié en alguna aplicación, para permitir que la implementación sea lo más flexible posible.

Existen otras alternativas en cuanto a manejo de usuarios y servicios, como la virtualización de los mismos, pero como estoy tratando de ser lo más genérico posible, las he descartado, pensando en instalaciones básicas, desde cero, y destinadas antes que nada a usuarios noveles. De todas maneras, los conceptos aquí vertidos no persiguen, como ya aclaré, ser una guía completa de seguridad (ya las hay, y mucho mejores), sino un compendio de prácticas recomendables.

Dichas estas palabras preliminares, comencemos con el trabajo…

SEGURIDAD en LINUX

Por Luis H. Otegui

De 0 a 100 en 5 notas

Primera Parte: En el principio...

… había un disco rígido, vacío -o quizá con otro sistema operativo viviendo en él. Luego, decidimos instalar Linux, y convertirnos en un *deus in machina*, el súper usuario, **root**. Y, a partir de ese momento, comenzamos con un camino que puede ser tan tortuoso -y tan interesante- como nosotros queramos.

Como dije en la introducción, no me ceñiré a las características de ninguna distribución en particular. Trataré de focalizarme en los puntos en común que tienen todas, es decir, las que de alguna manera resumen la *esencia* de Linux. Que cada cual elija la distro que mejor le venga en gana, sea por facilidad de uso, seguridad, o hasta por disponibilidad de los CD o DVD de instalación.

Como norma, tratemos de conseguir, sea cual sea la distribución que elijamos, la última versión, y de leer además en el sitio que la cobija, qué vulnerabilidades se le han encontrado, o qué actualizaciones son estrictamente necesarias, y tomemos nota. Nos ahorrará trabajo más adelante.

Las instalaciones de las distintas *distros* son más o menos amigables. Pero todas tienen un punto en común, crítico a la hora de decidir la performance y facilitarnos las tareas de asegurar nuestra máquina en el futuro: el particionado del disco. De acuerdo al perfil que le deseemos dar a nuestra máquina, deberemos decidir el tamaño de las distintas particiones. ¿vamos a instalar nuestra estación de trabajo?¿será este un servidor de correo?¿o quizá de Web?¿un proxy-caché?¿un servidor de archivos? Cada variante tiene sus vericuetos. Por ejemplo, si vamos a instalar un servidor de correo, en la forma más simple, deberemos dejar una partición /var proporcionalmente más grande que el resto (siempre pensando en función de los usuarios de correo actuales y teniendo en cuenta prospecciones futuras de crecimiento). Al igual que si instalamos un servidor de Web, ya que en ésta partición vivirán las páginas web alojadas. Un *fileserver*, o una estación de trabajo multiusuario, nos demandarán un particionado que coloque al /home como el sector más grande del disco.

Ahora bien, muchos me dirán que ven como la razón más importante para dimensionar de esta forma las particiones el evitar que alguna se nos llene, y termine colgando la máquina. Hay una más importante, y que adelanté en el párrafo anterior: de esta forma estamos definiendo dónde van a **vivir** preponderantemente los usuarios -sean reales o virtuales- del sistema. Y de esta forma, podremos controlar mejor las restricciones que sobre ellos decidamos imponer. Ya lo dije muchas veces, suena feo, y hasta fascista, pero hay que darle a cada usuario sólo los privilegios que necesita para hacer su trabajo. Y así, el nuestro será más fácil.

Un punto importante al que no se le suele prestar atención es al usuario normal que se nos pide generar durante las instalaciones. El mismo es una parte crucial de nuestro sistema. Supongamos que se nos ocurre instalar una aplicación que no está disponible como paquete instalable para nuestra distribución, sino en forma de código fuente. Este código fuente suele venir acompañado de un script llamado **configure**, que se encargará de configurar los parámetros necesarios para que el comando **make** nos devuelva un programa ejecutable en nuestro sistema, averiguando la versión del compilador de C, librerías asociadas, kernel, etc., que existen en nuestro Linux. Normalmente, uno descarga el paquete de fuente comprimido, lo descomprime, y sigue los pasos arriba mencionados. Todo como el súper usuario, mejor conocido como **root**. El problema es que si alguien cambió el paquete de software que nosotros con tanta confianza descargamos, al ejecutar los comandos ***configure*** y ***make*** como ***root***, nos podemos encontrar con la sorpresa de instalar una utilidad de tipo *back orifice*, o algún otro código dañino, que podría utilizar los privilegios de nuestro súper usuario para instalarse y tomar control de nuestro sistema. Es por esto que es muy recomendable echar mano al súper usuario sólo en determinadas ocasiones, como cuando hemos de instalar, configurar o actualizar algún paquete (no código fuente, salvo en la etapa de ***make install***), o para realizar chequeos de seguridad en el sistema. Para lo demás, aunque los únicos que utilicemos el sistema seamos nosotros, nos conviene movernos con nuestro usuario normal.

Y ya que de creación de usuarios estamos hablando, debemos dedicar un párrafo a las contraseñas que utilizamos, y a la política que estableceremos sobre ellas. Mucha gente no se toma el tiempo suficiente a la hora de generar su contraseña. O no piensan que la misma sea relevante. Pero si nuestro sistema va a estar expuesto a la red, o a varios usuarios, es necesario educar a los mismos -y educarnos a nuestra vez- sobre ciertos parámetros básicos. En primer lugar, las contraseñas no deben ser simples. A modo de ejemplo, podemos citar un estudio realizado en los Estados Unidos. El mismo reveló que en los primeros lugares de las listas de contraseñas más usadas están los apodos personales, el nombre de la mascota, el número de teléfono o documento, y (aunque parezca mentira) la palabra "Dios" ("*God*", en ingles). Una política de contraseñas mínimamente aceptable debería incluir contraseñas complejas, formadas por letras y números, y con mayúsculas y minúsculas. La queja más común de los usuarios a este respecto es que son difíciles de recordar. Una solución posible es crear las contraseñas asociadas a reglas mnemotécnicas. Por ejemplo, para el encargado de ventas que se llama Juan y trabaja en la compañía desde el 85, podríamos crear la contraseña "ElmdJqtdde85", que se relaciona con la frase "**E**s **l**a **m**áquina **d**e **J**uan **q**ue **t**rabaja **d**esde **e**l **85**".




FOTO: (c) JUPITERIMAGES, and its Licensors. All Rights Reserved

El primer arranque

Finalizada la instalación de nuestro Linux, deberemos echar mano de alguna herramienta de actualización, para poder descargar las últimas versiones de aquellos paquetes que pudieran presentar alguna vulnerabilidad. Linux es un sistema operativo en constante evolución, y los mantenedores de las distintas distribuciones deben elegir una versión de cada paquete de software para incluir en los las imágenes de los instaladores. Pero eso no significa que los mismos dejen de evolucionar. Y hay ciertos paquetes que resultan críticos a la hora de prevenir fallos en el sistema, mejorar su rendimiento, o, en el caso que nos ocupa, evitar que alguien se tome atribuciones superiores a las que posee. Sea un usuario local, sea un atacante externo. Aquí es donde leer los anuncios de noticias del sitio de la distribución que hemos elegido nos va a servir. Seamos realistas, hoy por hoy, es necesario tener nuestro sistema enchufado a la red de redes, para que el mismo funcione correctamente. Más aún, me atrevería a decir que el sino de un sistema Linux reside en estar conectado, y compartir información.

En la mayoría de las distribuciones nos encontramos con varias versiones de un paquete, en función de variables tales como la madurez del código fuente y su nivel de integración con el núcleo y el resto de las aplicaciones empacadas junto a él. Normalmente, disponemos de paquetes de tipo inestable (unstable), en evaluación (testing), estables (stable), y aquellos generados por usuarios que sin ser miembros de la comunidad de desarrollo, deciden o bien convertir en paquetes instalables aplicaciones que sólo están disponibles como código fuente, o generar sus propios paquetes, sea con el fin que sea.

De más está decir que si descargamos paquetes para instalar y/o actualizar, debemos cerciorarnos de que el servidor desde el cual los obtenemos sea el que debe ser (es decir, no somos víctimas del *spoofing*), y de que los paquetes hagan lo que dicen hacer (las comprobaciones vía md5 suelen ser muy útiles a este respecto). Lo recomendable, a menos que sepamos muy bien lo que estamos haciendo, es mantenernos dentro de la línea de paquetes estables. Esto tiene el riesgo asociado de deber quedarnos con aplicaciones un poco "viejitas", por lo cual deberemos estar bien despiertos, y chequear si a las mismas no se les ha detectado alguna clase de vulnerabilidad. Para esto, mi consejo personal es suscribirse a algún servicio de evaluación de vulnerabilidades, como por ejemplo, www.securityfocus.com.

Más hoy es menos mañana

Me refiero con este título al trabajo a realizar en el equipo para garantizar su integridad de cara al futuro. Llegados a este punto, con nuestro sistema en funciones, actualizado a lo último, y habiendo decidido cual será su tarea, deberemos dedicarnos a desactivar todos aquellos programas, servicios y/o demonios que no sean esenciales para el funcionamiento del mismo. Casi todos los servicios que se activan al arranque en un Linux típico corren o bien en modo *standalone* (vía un *daemon*, o demonio), o bien vía alguno de los súper servidores, ***inetd***, o su reemplazo, ***xinetd***. Cuántos servicios deberemos desactivar dependerá de la función del sistema, y de la distribución que hayamos elegido (algunas activan por defecto muchos servicios que, en general, no son necesarios). Algunas incluyen utilidades para realizar estos cambios mediante alguna interfaz, sea vía la consola gráfica o vía la línea de comandos, y en otras, deberemos borrar los enlaces simbólicos de los directorios de arranque (los conocidos rcX.d, donde X es el nivel de arranque por defecto del sistema).

Una vez que nos hemos deshecho de las utilidades que corrían espúreamente en nuestro joven sistema, lo que nos queda es **configurar correctamente** aquellas que posibilitarán que el mismo cumpla con la función que le hemos asignado.

¿Por qué elegimos deliberadamente no activar al inicio aquellas aplicaciones que no nos sirven? Por varias razones. La primera, conservar los preciados recursos de nuestro sistema. La segunda, cerrar puertos que de otra manera estarían abiertos, brindado cuando menos alguna información acerca de nuestro sistema a cualquiera que nos analice remotamente. Y tercero, porque de esa forma deberemos buscar periódicamente menos

Lecturas Adicionales

-The US Department Of Energy,CIAC (Computer Incident Advisory Capability):
http://ciac.llnl.gov/ciac/index.html

-CERT (Computer Emergency Response Team) vendor security sites:
http://www.cert.org/

-BugTraq:
http://www.securityfocus.com/forums/bugtraq/intro.html

noticias sobre vulnerabilidades de aplicaciones. Además el *script* del *firewall* se nos hará más simple cuantos menos puertos haya abiertos.

La imaginación al poder

Volvamos a lo que dije dos párrafos atrás. ¿A qué me refiero por "configurar correctamente" una aplicación? Bueno, en general, cada aplicación viene con una primera configuración por defecto. Es la mínima necesaria para que corra. Normalmente, necesitará de nuestro intelecto -y de nuestros dedos- para convertirse en un servicio útil de nuestro sistema.

Aquí rescato una frase de Mick Bauer, que ya cité en una nota anterior: *"el problema es que los usuarios de Linux, al igual que los de Windows, se concentran más en lograr que sus sistemas hagan lo que ellos quieren que en la seguridad de los mismos"*. ¿Cómo se traduce esto? Los desarrolladores de una aplicación hacen todo lo posible para que la misma sea tan segura como se pueda. Pero puede pasar que en el apuro por que la misma haga lo que nosotros queremos que haga, por ejemplo, relajemos alguna configuración, cambiemos algún permiso sobre un directorio, o el usuario bajo el cual corre por defecto. Habrá que evaluar qué posibles consecuencias tendrá en el sistema cualquiera de estos cambios. Y, al revés de como tenemos costumbre de trabajar, **leer la documentación de forma exhaustiva** antes de realizar cualquier cambio.

Normalmente, nos apuraremos por lograr que la cosa "salga andando" echando mano a recursos tan dispares como HOWTOS, listas de correo, la palabra de algún amigo o colega con más experiencia que nosotros, o hasta algún rezo velado y en voz baja (esto último está acompañado por lo general por cambios aleatorios y sin razón en permisos, usuarios, parámetros de arranque, etc.). Y cuando la cosa camine por sí sola, respiraremos tranquilos, y pasaremos a atacar el siguiente desafío. Y ahí es cuando metemos la pata.

A ver si lo dejo suficientemente claro: Si realizamos cualquier cambio (y más en el último caso del párrafo de arriba), deberemos evaluar, como ya dije antes, las posibles consecuencias para las demás aplicaciones de nuestro sistema. Más en el caso en que tengamos dos o mas aplicaciones interdependientes, o que intercambien información, como en los casos de un *webwserver* y una base de datos, o un directorio LDAP y un servidor de correo o SAMBA. Más aún si estas aplicaciones corren en distintos *hosts*. Compatibilizar permisos no es una tarea fácil. Pero más vale encararla desde el principio de la vida de nuestro sistema. Nos ahorrará trabajo a posteriori, como ya dije.

Una vez logrado el tan deseado equilibrio de las aplicaciones a correr, deberemos barajar la posibilidad de que los usuarios interactúen con ellas, sea de forma local (sentándose en la consola), o por las varias formas de acceso remoto disponibles. Y cuando digo acceso remoto, me refiero tanto al que se realiza vía *shells* (*rsh, telnet, ssh*), como al que se da vía alguna aplicación específica, como las conexiones a bases de datos, servidores web, o



de correo. En cada caso específico deberemos pensar que habrá que crear uno o más usuarios reales, y qué privilegios tendrán. Si los usuarios van a enviar y recibir su correo por medio del sistema y de forma remota, por ejemplo, no hará falta que los shells que figuren en sus entradas del archivo /etc/passwd sean reales, sino que podremos sustituirlos por alguno de los *fake shells* que figuran en el archivo /etc/shells. De esta forma, estaremos evitando que obtengan acceso a la consola.

Y si necesitamos que un usuario modifique los contenidos de un sitio web que alojamos, deberemos constatar que el mismo forme parte de los grupos correctos, tenga acceso de lectura y escritura a los directorios pertinentes, y a ninguno más.

Generalmente, el lograr la correcta interacción del sistema con los usuarios nos tomará más o menos tiempo en función de nuestra experiencia, y del material de consulta que hayamos acumulado. En algunos casos será una tarea ardua, tanto peor cuantos más servicios deseemos correr sobre el sistema. Pero, no me canso de repetirlo, es tiempo bien invertido.

Puertas abiertas, puertas cerradas

Una vez que hemos compatibilizado, en un entorno de prueba, el funcionamiento del sistema con la actividad de los usuarios, debemos comenzar a realizar una labor de sastre con el firewall. Dependiendo de nuestra pericia y conocimiento del filtro de paquetes estándar de Linux, *Netfilter*, podremos generar los *scripts* pertinentes a mano, o mediante alguna utilidad o sistema de configuración.

Para llegar a que el firewall funcione *correctamente* -y por *correctamente* me refiero a que deje pasar únicamente lo que necesitamos que pase, y nada más- la aproximación más simple consiste en enumerar los servicios que tenemos abiertos, y las conexiones que deseamos establecer desde y hacia nuestro sistema, y desde y hacia el resto del mundo. En mi opinión, lo más simple y productivo a la larga es generar un firewall cuya política por defecto sea la denegación de la conexión (política por defecto DROP). Nos llevará más tiempo de configuración, habrá más idas y vueltas, y si no sabemos mucho de IPTables se nos puede hacer un poco engorroso, pero es más simple de mantener, y más seguro.

Tarea fina, casi concluida

Bueno, ahora ya podemos considerar que ya tenemos un sistema Linux listo para ser utilizado. Para mucha la gente, varios párrafos más atrás esto ya era evidente. Pero la pregunta que deberían hacerse quienes piensen así, inevitablemente, es "¿y qué tan seguro es?". Trabajando de la manera que he resumido nos aseguraremos de tener un sistema que no sólo haga lo que nosotros queremos, sino que además, lo haga sin poner en peligro su propia integridad.

Más arriba dije que Linux es un sistema operativo "vivo", en el sentido de que está en permanente evolución. Nuestro Linux recién instalado apenas se ha asomado a la vida. E igual que un padre con sus vástagos, deberemos velar por su integridad en una forma más o menos constante. Vale decir, no podemos instalarlo y esperar que sea invulnerable, o que funcione correctamente a perpetuidad. Está pensado para minimizar las tareas de administración y mantenimiento, no para hacerlas desaparecer. Por eso es importante sistematizar el proceso de instalación, y realizar chequeos periódicos. A lo dice el refrán, el ojo del dueño engorda el ganado.

Lo que vendrá

En el artículo siguiente analizaremos los distintos tipos de firewalls a implementar de acuerdo al uso al que se destinará el sistema, la interacción de los firewalls de varios hosts, y las distintas aproximaciones a los exámenes periódicos que será menester realizarle para asegurarnos de que continúe funcionando como deseamos. ■

CES 2006
El futuro dijo presente

David A. Yanover
Director de www.MasterMagazine.info

El mercado tecnológico ha visto cómo se ha establecido, en este último tiempo, el negocio de las búsquedas como un espacio clave de presencia y alcance sobre la sociedad. Sus históricos jugadores, más allá de los pocos años de vida que tienen en este ámbito, son MSN (de Microsoft), Yahoo! y el hasta ahora imbatible Google, que tiene a sus pies a la mayoría de la gente. Estas tres marcas son los grandes motores de Internet, porque se encargan de asistir a millones de navegantes, para que tengan un buen viaje virtual, alcanzándoles la información que necesitan.

Otra forma de llegar al usuario es, por lo que se observó en CES 2006, el entretenimiento digital. Microsoft mostró su brillante Xbox 360, y Sony se enorgulleció de su pequeña y poderosa PSP. Por su parte, la telefonía celular, cada vez más compleja e inteligente, ya es parte de nuestras vidas, y cada empresa está interesada en integrar sus soluciones a estos dispositivos personales, que lo siguen a uno a donde quiera que vaya. Todos estos caminos buscan llevar la tecnología a la persona, para que ésta la adapte a su vida, a su hogar. Para encontrar las respuestas a varias de las tendencias que nos depara este 2006 fue necesario echar un vistazo a lo que sucedió en Las Vegas a principios de enero, y de este modo advertir las pautas de un futuro cada vez más presente en la vida cotidiana.





Microsoft mejora la imagen digital

Las palabras de Bill Gates giraron en torno a la vida digital, comprendiendo al usuario común, visualizando el modo en que la tecnología forma parte su rutina diaria, facilitándole tareas y ayudándolo a relacionarse.

Windows Vista fue una vez una de las estrellas de Las Vegas -"nuestro producto más importante", afirmó Bill Gates-. A pesar de que el nuevo sistema operativo estará saliendo al mercado a fines de este año, genera mucha expectativa, siendo la base de los próximos desarrollos de la compañía.

Para la presentación de la consola de videojuegos de nueva generación, Xbox 360, Bill Gates se enfrentó a Steve Ballmer (Presidente de Microsoft) en el título Fight Night Round 3, que simula enfrentamientos de boxeo logrando un nivel de detalle impresionante. Steve Ballmer le advirtió a su oponente, "estuve preparándome durante 30 años para esta oportunidad". El juego y sus jugadores, más allá de darle color a la conferencia, evidenciaron el profundo esfuerzo de Microsoft por continuar capturando parte del mercado de los videojuegos. El gran poder de su máquina quedó en evidencia, haciendo uso del formato de discos HD-DVD lista para enfrentarse a la Sony Playstation 3 y a la Nintendo Revolution.

"Pienso que el 2006 será un gran año para el estilo

de vida digital", decía Bill Gates sobre el cierre de su conferencia, apoyándose en dos tendencias. Por un lado, la alta definición del entretenimiento electrónico, producido tanto por Xbox 360 como a través de los sistemas y aplicaciones informáticas, como el Media Center, ahora capaces de llevar una mayor experiencia en video y audio. Por el otro lado, Bill Gates destacó la necesidad de establecer relaciones con empresas de toda clase, y prueba de este pensamiento han sido las numerosas alianzas presentadas por Microsoft (y también del resto de las compañías) en CES 2006.

Yahoo! en medio de una Misión Imposible

Mientras Terry Semel, CEO de Yahoo!, intentaba mostrar una previa de la futura película Misión Imposible III a través del novedoso Yahoo Go TV (que hace posible acceder a contenidos multimedia desde un televisor conectado a una PC convencional), la conexión a Internet falló, y Tom Cruse tuvo que salir al rescate al ser invitado por el directivo de Yahoo!. Mientras tanto, los ejecutivos e ingenieros de Yahoo! sufrían por el pequeño problema técnico. Microsoft recibió algunos chistes, que ayudaron a relajar el clima. "Ya sabemos sobre que software está corriendo", se le escapó a Terry Semel, mientras muchos de los presentes se divertían a raíz de la irónica situación, dado el contexto. Cerca, estaba también Paul Otellini, ingeniero de Intel, quien se había subido al escenario para formar parte de esta presentación en la que estaban involucrados los procesadores Viiv de Intel. Finalmente, pudo apreciarse el trailer de la película, y apenas terminó una persona del público gritó, "pásenla de nuevo", a lo que Tom Cruise asintió para "poner a prueba la velocidad de respuesta del sistema", ya tras haber superado la falla de conectividad. Una anécdota divertida que muestra que los tradicionales errores, ya sea en la oficina o en el hogar, también son sufridos por los ingenieros y programadores más avanzados, y en la sede de mayor innovación tecnológica.
Luego, Ellen DeGeneres recibió el pase de Terry Semel para continuar la conferencia, haciendo reír aún más a los espectadores. Pero no fue lo único que tuvo esta presentación, porque se mostró Yahoo Go Mobile, un sistema que permite accesos a Internet desde dispositivos móviles, permitiendo la lectura de correos electrónicos, la visualización de fotografías, y el uso de clientes de mensajería, entre otras utilidades y servicios de Yahoo!.

El imperio de Google

El buscador era una de las apuestas más fuertes de este CES 2006, y sus responsables cumplieron con las expectativas. Las novedades del motor de búsqueda fueron desarrolladas por el propio Larry Page, Co-Fundador y Co-Presidente de Google. El joven empresario contó con las visitas al escenario del actor Robin Williams, la estrella de la NBA Kenny Smith y Leslie Moonves, directivo del gran medio de comunicación norteamericano CBS. Estos dos últimos acompañaron el lanzamiento de Google Video Store, que consiste en la venta de videos a través de Internet. El nuevo desarrollo de Google tiene el apoyo de numerosas empresas relacionadas con la música, el espectáculo, el deporte y el entretenimiento en general. Google Video Store comenzó su camino con un catálogo muy amplio de opciones para los navegantes en el que figuraron las series televisivas de la CBS.
No obstante, la primera gran mención se la llevo Stanley, un robot de cuatro ruedas desarrollado en la Universidad de Stanford (donde se dieron los orígenes de Google). Como símbolo de inspiración de lo que la ingeniería es capaz de hacer, Larry Page continuó su charla.
Se mostraron imágenes del Google Live Query, que consiste en una pantalla ubicada en la sede central del motor de búsqueda que muestra las consultas que hacen los usuarios en tiempo real, y se hizo énfasis en la innovadora portátil de 100 dólares, proyecto que tiene por objetivo llegar a sectores desprotegidos del mundo y del cual Google es responsable del Thin Client (sistema que ayuda a ofrecer potentes aplicaciones de Internet más allá de los escasos recursos del equipo, dado que se conecta con un servidor central para proveer las ciertas funciones). La pantalla principal que capturaba los ojos de los presentes no olvidó mostrar Google Earth, que hizo un acercamiento sobre la Torre Eiffel de París para luego trasladarse al propio lugar donde se desarrollaba el evento. Google Talk, el cliente de mensajería instantánea, y Google Local Mobile, edición del buscador pensada para dispositivos móviles, también tuvieron sus espacios; era un desarrollo tras otro, que capitulaba los principales lanzamientos de Google de los últimos tiempos. Por último, se anunció la salida de Google Pack, que encierra muchas de las aplicaciones ya mencionadas en una oferta de descarga gratuita.

Electrónica de avanzada

Sir Howard Stringer, CEO de Sony, hizo una pasarela de los más recientes productos de la empresa, haciendo especial hincapié en la consola portátil de juegos PSP, y el Sony Reader, una plataforma de libro electrónico capaz de almacenar cientos de títulos. Mientras que Paul Otellini, directivo de Intel, dio a conocer los innovadores procesadores Viiv, su empresa renovó su logo y visión reforzando su posición hacia el desarrollo del hogar digital. Para Otellini, "es el inicio de una nueva era en la televisión", a partir de las características que incorpora Intel a su gama de chips -que le permiten capturar imágenes de alta definición-, y al respaldo que muestran otros líderes de la industria por converger los distintos medios audiovisuales.

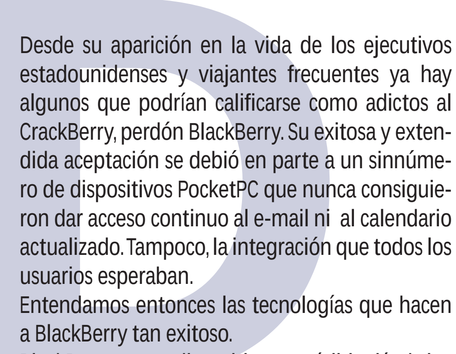
Para ver las conferencias desde Internet

http://www.cesweb.org/attendees/conferences/keynotes.asp


Bill Gates en la CES 2006, durante la presentación de las nuevas tecnologías que incorpora Windows Vista.

LA TECNOLOGÍA DETRÁS DE BLACKBERRY

Alejandro Cynowicz
Editor Técnico - Revista NEX IT Specialist



Desde su aparición en la vida de los ejecutivos estadounidenses y viajantes frecuentes ya hay algunos que podrían calificarse como adictos al CrackBerry, perdón BlackBerry. Su exitosa y extendida aceptación se debió en parte a un sinnúmero de dispositivos PocketPC que nunca consiguieron dar acceso continuo al e-mail ni al calendario actualizado. Tampoco, la integración que todos los usuarios esperaban.

Entendamos entonces las tecnologías que hacen a BlackBerry tan exitoso.

BlackBerry es un dispositivo portátil inalámbrico que soporta e-mail, telefonía móvil, mensajes de texto, navegación de Internet y otros servicios inalámbricos. Es fabricado por **Research In Motion** y ofrecido al público a través de empresas de telefonía. Su inserción en el mercado se centró en la compatibilidad con el correo electrónico.

Actualmente, Research In Motion se encuentra en una disputa por patentes acerca de este producto. Gracias a su incremento en popularidad, los BlackBerry son usados también en escenarios sociales, más allá del sector profesional, para agendar compromisos con conocidos, usar su libreta de contactos, etc. La facilidad de tipeo y envío de no sólo e-mails, sino también de mensajes de texto SMS (Short Massages Services), nos permite responder rápidamente un correo electrónico escribiendo un SMS aunque el remitente del primero lo haya escrito desde un teléfono celular y no tenga un BlackBerry.

Durante 2006 serán habilitados los primeros clientes BlackBerry en Argentina. El arribo de esta



Perfil de RIM: *Research In Motion Limited es diseñadora y fabricante líder de soluciones inalámbricas innovadoras para el mercado mundial de comunicaciones móviles. A través del desarrollo de hardware, software y servicios integrados que soportan múltiples estándares de redes wireless, RIM provee plataformas y soluciones para acceso ininterrumpido a información que necesite actualización inmediata, incluyendo correo electrónico, telefonía, mensajería SMS, Internet y aplicaciones basadas en Intranet. La tecnología de RIM también les permite a una amplia gama de desarrolladores y fabricantes mejorar sus productos y servicios con conectividad inalámbrica a sus datos.*
Los galardonados productos, servicios y tecnologías embebidas son usados por miles de organizaciones alrededor del mundo, algunos de ellos son: la plataforma inalámbrica BlackBerry, la línea de productos RIM Wireless Handheld, herramientas de desarrollo de software, radio-módems y acuerdos de licencias de software/hardware. Fundada en 1984 y con base en Waterloo, Ontario, Canadá, RIM tiene oficinas en Norte América, Europa, y Asia. Está enlistada en el mercado de valores Nasdaq (Nasdaq: RIMM) y en el Toronto Stock Exchange (TSX: RIM).

tecnología, que apunta a los ejecutivos, les permitirá optimizar su productividad y pondrá al alcance del mundo corporativo el acceso remoto a los datos en forma **inalámbrica, rápida y segura**.
Aquí veremos la tecnología detrás de la infraestructura que permite a los BlackBerry comunicase en grande, ocupando un espacio pequeño.

Dos gamas de dispositivos

- **BlackBerry Business Phones:** Proveen la mejor experiencia para el uso de e-mail y datos inalámbricos, para usuarios que prefieran un aparato con un diseño más pequeño. Ofrecen funcionalidad completa con las características de BlackBerry como ser el teclado con tecnología SureType™ y Bluetooth.
- **BlackBerry Handhelds:** Cada handheld, tiene un teclado QWERTY, una rueda lateral para usar con el pulgar, pantalla de fácil lectura retro-iluminada, interfaz de menús intuitiva e integrada a las aplicaciones de software.

Entre las características generales que comparten la mayoría de los dispositivos BlackBerry, podemos destacar los siguientes:
- Pantalla Color de LCD
- Wi-Fi 802.11b para datos y VOIP (Voice Over IP)
- GSM (Group Special Mobile) / GPRS (General Packet Radio Service)
- WAP (Wireless Application Protocol), websites programados en WML y HTML
- 3G - CDMA2000
- Teclado QWERTY.
- Sistema Operativo: BlackBerry OS 4

BlackBerry Enterprise Server

Esta tecnología, provee características avanzadas de seguridad a la vez que combina y sincroniza el correo electrónico, calendario y contactos, con el cliente de correo de la PC. Para acceder al e-mail corporativo en forma wireless a través de BlackBerry Enterprise Server (BES), la empresa debe instalar el software BES en su Server corporativo. También les provee a las handhelds, conectividad TCP/IP que les llega a través de un Proxy gracias un componente llamado **"Mobile Data Service"** (MDS). Ésto permite el desarrollo de aplicaciones personalizadas utilizando *streams* de datos en dispositivos BlackBerry basados en la plataforma **J2ME** (Java2 Micro Edition)de Sun Microsystems. Dicho software representa un gasto adicional (u$s 3,999 por servidor con 20 clientes) y se vende por separado.
La conectividad universal de la infraestructura BES/MDS es uno de los aspectos más valiosos del producto de Research In Motion.
En las más recientes versiones de la plataforma BlackBerry, el MDS ya no es un requisito necesario para acceder a datos inalámbricamente.
A partir de la versión 4.0 de su sistema operativo, las handhelds BlackBerry pueden acceder a Internet (acceso vía TCP/IP) sin MDS. El BES/MDS es aun requerido para acceso seguro a datos y correo. En versiones anteriores a la 3.8, prescindiendo del BES/MDS sólo podía accederse al e-mail y WAP. Todos los datos (e-mail y tráfico MDS) que viajan entre el BlackBerry y un BlackBerry Enterprise Server son encriptados usando el algoritmo **Triple DES**.
Según sea el modelo específico de BlackBerry, el soporte multi-banda puede incluir las siguientes:
- GSM 850/900
- Dcs 1800
- Pcs 1900

Las BlackBerry modernas incorporan un procesador **ARM 7** ó **9** y los primeros modelos (el 950 y el 957) usan **Intel 80386**. Recientemente anunciaron que los próximos modelos tendrán el procesador celular **Intel XScale PXA9xx** (code name: "Hermon") con velocidades que superan los 300 Mhz.
Una pregunta que surge es si Exchange Server 2003 con Service Pack 2 (SP2) junto con **Windows Mobile 5.0 Messaging and Security Pack** hará a Exchange competitivo frente a **RIM** y otras soluciones móviles. Pero ésto será tema de otro artículo. ■



La elección del nombre BlackBerry, fue casual e impulsiva; RIM se decidió a adoptarlo tras varias semanas de trabajo de la firma californiana ***Lexicon Branding Inc****. que se dedica a crear marcas, logotipos y slogans que sean pegadizos y familiares para los consumidores. Le dio nombre al microprocesador* ***Pentium*** *de* Intel, *y a la* **PowerBook** de Apple. *Uno de los expertos en nombres en Lexicon, pensó que los botones en miniatura del portátil de la empresa canadiense, se parecían a las pequeñas semillas en una frutilla. Un lingüista en la firma pensó que el sonido "straw" (de* strawberry, *frutilla) sonaba muy lento. Otra persona sugirió* **BlackBerry**. *Y así es como lo conocemos hoy.*



Wireless MESH NETWORKING
IEEE 802.11s

Carlos Vaughn O´Connor

Wireless Mesh Networking es una tecnología muy nueva y con grandes posibilidades de aplicación en defensa, acceso a Internet en áreas metropolitanas, redes que permanecen poco tiempo activas (por ejemplo, recuperación en desastres o centros de convenciones), edificios donde resulta difícil/cara la implementación de una red cableada (museos por ejemplo), terrenos poco amigables y áreas rurales con grandes costos para implementar redes convencionales.

Representa un tipo de infraestructura inalámbrica descentralizada, relativamente económica, muy fiable y resistente. Cada nodo necesita transmitir tan lejos como el próximo nodo. Los nodos actúan como repetidores de datos de nodos cercanos a otros equivalentes pero más lejanos. De este modo es posible implementar redes que pueden abarcar grandes distancias. La fiabilidad y resistencia se basa en el hecho que cada nodo se haya conectado a varios otros. Si un nodo cae (falla de hardware u otra causa) sus vecinos simplemente buscan otra ruta. Es posible mejorar la implementación de forma muy simple, agregando más nodos. Cada nodo puede ser un dispositivo fijo o móvil. Las figuras 1 y 2 ejemplifican una red Wireless Mesh.

Es posible distinguir 2 tipos de arquitecturas de Mesh Networking: i) redes client-mesh, donde los dispositivos de usuarios finales (tales como PCs, PDAs o laptops) participan en el ruteo de paquetes. Esta redes son "infrastructure-less" (no tienen infraestructura) en el sentido siguiente: la operación de un client-mesh no está administrado o monitoreado por un proveedor de servicios (ISP). ii) redes en modo infraestructura ("Infrastructure-Mesh"), donde los usuarios finales no participan en el relay de los paquetes. Existen entonces access points inalámbricos no connectados a un backbone de cable sino que por un lado dan acceso a los usuarios finales a través de algunas de sus interfaces de radio y que entre ellos hacen relay de paquetes usando las otras interfaces.

Microsoft y barrios auto-organizados usando Wireless Mesh Networking.

Grupos de investigación de Microsoft localizados en Redmond, Cambridge, UK y Silicon Valley trabajan en tecnologías capaces de permitir a los vecinos conectar sus redes hogareñas. Hay muchas ventajas para realizar tal conectividad y formar una comunidad a través de mesh networking. Por ejemplo, cuando un suficiente número de vecinos participa en hacer forward los paquetes de los otros, no es necesario tener un punto de acceso a Internet individual. Por el contrario, esta infraestructura permitiría compartir una salida a Internet común, reduciendo costos dramáticamente. Los paquetes encontrarían en forma dinámica su ruta ruteandose en el nodo de cada vecino hasta alcanzar el gateway común a Internet (ver figura 1.). Otra ventaja estaría en poder realizar backups en forma cooperativa despreocupándose de perder la información en sus discos individuales. Una tercera ventaja sería que el tráfico local queda confinado permitiendo una diseminación más rápida y sencilla de información en un "cache" de interés a la comunidad.

Sin embargo, para poder realizar lo anterior quedan problemas por resolver: aumento de la capacidad y rango de cobertura, privacidad y seguridad, ruteo multi-path auto estabilizante, auto configuración, equidad en uso del ancho de banda, etc.

Varios test-beds en los propios laboratorios y en complejos habitacionales han servido como pruebas pilotos. Si desea conocer más sobre estas interesantes experiencias vea: http://research.microsoft.com/mesh

Figura 2

CISCO y Wireless Mesh Networking.

La propuesta de CISCO de Wireless Mesh Networking provee una solución al acceso Wi-Fi wireless a escala de campus o redes-metropolitanas fundamentalmente con access Points inalámbricos localizados en el exterior (por ejemplo afuera de los edificios, en postes de luz, postes de semáforos).

La solución de CISCO se basa en routing wireless, donde links dinámicos son creados entre los diferentes acces points eliminando la necesidad de una conexión alámbrica en cada uno de ellos. Utiliza un Protocolo (aún a la espera del patentamiento) llamado "Adaptive Wireless Path Protocol", diseñado especialmente para redes inalámbricas. La red se auto-optimiza (self-optimizes) y auto-cura (self-heals), lo que le da resistencia a condiciones de conectividad cambiantes. De este modo se minimizan los costos de puesta en funcionamiento y administración.

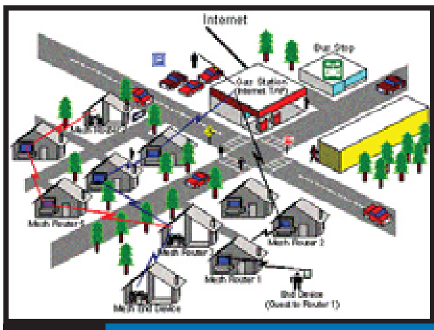
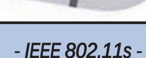


Figura 1



- IEEE 802.11s -

802.11 es un conjunto de estándares dado por la IEEE (Institute of Electrical and Electronics Engineers) que gobiernan los métodos de transmisión en redes inalámbricas. Son usadas muy comúnmente hoy en sus versiones 802.11a. , 802.11b y 802.11g.

802.11s es el estándar para ESS Mesh Networking y está aún sin aprobar. Especifica una extensión al MAC del IEEE 802.11 de modo de resolver problemas de interoperabilidad definiendo una arquitectura y protocolo que soporta tanto broadcast/multicast y unicast usando métricas "radio-aware" (basadas en ondas de radio), sobre topologías "multi-hop" auto configurables.

La demanda para acceso inalámbrico con access points localizados en el exterior ha ido aumentando. Hoy se cuenta con presupuestos más ajustados y recursos reducidos.. Por tanto la respuesta al WLAN (Wireless LAN) debe tomar ventaja de las herramientas, conocimiento y recursos de red existentes.

La figura 2 nos muestra una típica instalación. Los productos insignia en este tipo de infraestructura pertenecen a la serie: Cisco Airnonet 1500.

Varias grandes áreas metropolitanas ya cuentan con soluciones como esta.

Solo es cuestión de dejar volar la imaginación para entender la cantidad de aplicaciones posibles una vez cubiertas estas grandes áreas.

Lecturas Adicionales

http://research.microsoft.com/mesh
http://www.cisco.com/application/
http://www.motorola.com/





"Con los Spywares, Spams, Virus, Phishing, Troyanos, la navegación web y la productividad de mi empresa ya no son lo que eran. **Finalmente, una solución resuelve esta problemática de forma definitiva".**

Presentamos **McAfee® Secure Internet Gateway,** el primer appliance de seguridad Web y de e-mail del mercado, totalmente integrado. **McAfee SIG**, es parte de la familia de appliances **McAfee Secure Content Management**, y ofrece protección amplia contra spywares, spams, contenidos inadecuados de la Web, ataques de phishing, virus conocidos, worms y caballos de Troya. Es una solución simple y accesible que puede ser instalada con facilidad y prácticamente no exige ningún mantenimiento, ayudando a proteger los recursos de la empresa, aumentar la productividad de los empleados, reducir la eventual responsabilidad corporativa y el costo total de propiedad.

Visite http://www.mcafee.com/



McAfee® Secure Internet Gateway

Para adquirir este producto, contáctenos por email a: **ventas_argentina@mcafee.com** o por teléfono al **(011) 5166-3446/47**

SMB

Cómo la SEGURIDAD puede dispararnos un TIRO POR LA CULATA

Jesper M. Johansson
Enterprise Security Architect

Parte 1



Hace un tiempo atrás me tomé una pausa en la escritura de estos artículos. Ahora estoy de vuelta y pensé que sería divertido continuar los temas de seguridad, que comenzamos a hablar en la serie de "mitos de seguridad" y escribir acerca de algunas medidas beneficiosas que la gente toma por seguridad, pero que al final terminan rompiendo cosas. A diferencia en los mitos, de que hablaba en un nivel más alto, esta serie será más técnica. El objetivo es ayudarlo a comprender mejor algunas de las cosas que hacemos para aumentar la seguridad, y cómo pueden romper cosas a menos que seamos realmente cuidadosos en cómo las usamos.

No se en este momento cuantos de estos artículos escribiré, así que esta es la parte 1 de n. Este artículo trata sobre algo que por lo general es bueno pero que causa serios problemas porque la gente usualmente lo implementa incorrectamente: firma de mensajes del Server message Block (SMB). Por defecto, como veremos después, el único problema que debería ser causado por la firma de mensajes del SMB es que aquellos viejos sistemas corriendo Windows 9x no pueden conectarse a controlador de dominios (CD) de Windows Server 2003. (Windows 98 Second Edition y Windows Me soportan firma de mensajes del SMB por defecto, sistemas más viejos no lo hacen). Aun esto sólo debería afectar entornos en los que todavía no han cambiado sus máquinas corriendo Windows 9x, el 25% de todas las llamadas al Servicio de Soporte de Productos de Microsoft (SSP) son a causa de la firma de mensajes del SMB. Claramente esta configuración puede ser confusa para alguna gente, lo que lo hace un buen candidato para explicar en esta serie.

SMB Message Signing

El protocolo SMB (Server message Block), es lo que yace debajo de una red basada en Microsoft Windows. SMB es de hecho la versión de Microsoft de un estándar conocido como el Common Internet File System (CIFS). Otros sistemas implementan el mismo estándar, incluyendo notablemente el SAMBA y varios dispositivos de hardware como sistemas de almacenamiento "network attached". SMB es la base de todo el networking de Windows y es el protocolo usado para la compartir e imprimir archivos, la mayoría del tráfico de dominio, y una amplia gama de cosas indispensables en la redes Windows. SMB era hace años atrás, un modelo de amenaza muy diferente a lo que consideraríamos hoy. Por lo tanto, tiene pocas construcciones de seguridad incorporadas. En consecuencia, no fue ninguna sorpresa cuando "Hobbit" publicó en 1997 un trabájo de investigación llamado Common Insecurities Fail Scrutiny (Escrutinio De Fallas De Seguridad Comunes), destacando cuestiones de seguridad en SMB. Pronto se volvieron disponibles herramientas de ataque que tomaban ventaja de estas fallas de seguridad, incluyendo el ahora infame ataque de reflejo de SMB (SMB Reflection Attack).

Varios de los problemas con CIFS/SMB (de aquí en más, usaré tan sólo SMB para referirme al protocolo) eran ataques del tipo "hombre en el medio" (man-in-the-middle) donde un atacante consigue insertarse en la conversación y espiarla o modificar su contenido. Por ejemplo, un atacante podría escuchar la sesión de configuración del SMB entre un cliente legítimo y un servidor, capturar paquetes, y luego reproducirlos contra el servidor para establecer su propia conexión con éste.

El ataque de reflejo SMB es un tipo especial de ataque "hombre en el medio" donde el atacante y el servidor son la misma máquina. En el artículo "**Proteja Su Red Windows**", (habíamos explicado) explicamos el ataque de reflejo de la siguiente manera:

1. Máquina se A conecta a máquina B.
2. Máquina B envía un desafío a la máquina A.
3. Máquina A procesa la respuesta al desafío y lo envía a la máquina B.
4. La máquina B, habiendo hecho el mismo cálculo que A usando las credenciales que ha almacenado, ahora compara las respuestas con su propio valor calculado. Si las dos coinciden, la conexión es un éxito.



Ahora consideren este flujo: para que esto funcione, el atacante necesita convencer a la víctima para iniciar una conexión SMB al atacante. Este e-mail puede ser parte de un ataque de ingeniería social.

1.La víctima inicia una conexión con el atacante.
2.En este punto, el sistema del atacante se supone que envíe un desafío a la víctima para permitirle autenticarse.
3.La víctima genera un desafío para la conexión entrante del atacante y se la envía al atacante.
4.Atacante toma el desafío que recibió en el paso 3 y se lo envía a la víctima como desafió de la conexión que la víctima inició en el paso 2.
5.La víctima procesa la respuesta al desafío y la envía al atacante.
6.El atacante toma la respuesta recibida en el paso 5, y lo regresa a la víctima como respuesta a la conexión que había iniciado con la víctima en el paso 2.

Para más detalles sobre los pasos individuales, y cómo los atacantes los usan, ver "Proteja su red Windows", por Johansson y Riley.

En respuesta al paper de Hobbit, Microsoft agregó algunas características al SMB. Una de las características diseñadas para limitar estos ataques del tipo "Hombre en el medio" fue la Firma de Mensajes del SMB. Dicho sistema, firma paquetes SMB para asegurar que no puedan ser reproducidos contra un sistema diferente. La Firma de Mensajes de SMB tiene de hecho cuatro diferentes configuraciones. Nuevamente, como se explica en "Proteja su red Windows":

- Microsoft Network Client: Firmar digitalmente comunicaciones (Si el Server está de acuerdo) - Configura la Workstation de trabajo para que pida que sean firmados los mensajes en las peticiones salientes a Servers. Ésta es la única configuración de las cuatro que está habilitada por defecto. La ubicación de la configuración en el registro es: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation\parameters\EnableSecuritySignature. Si esta configuración es apagada, la Firma de Mensajes en este cliente está deshabilitada. Si está encendida, la Firma está activada.
- Microsoft Network Client: Firmar digitalmente comunicaciones (Siempre) - Configura la Workstation para que pida que sean firmadas las peticiones salientes a servers SMB. La configuración está almacenada en el registro en la siguiente dirección: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworksta-

tion\parameters\RequireSecuritySignature. Si esta configuración está activada, el cliente requiere que todo el tráfico sea firmado. Si está desactivado, la configuración de EnableSecuritySignature en el Workstation guía el comportamiento del cliente.

- Microsoft Network Server: Firmar digitalmente comunicaciones (si el cliente está de acuerdo). Hace que el servicio del servidor requiera la firma de mensajes en peticiones entrantes desde clientes SMB. Esta configuración está almacenada en el registro en:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\EnableSecuritySignature. Si este parámetro está desactivado, deshabilitará la firma de mensajes en el Server. Si se activa, también lo hará la firma.

- Microsoft Network Server: Firma digitalmente las comunicaciones (siempre) - configura el servicio del servidor para que requiera la firma de mensajes de SMB en peticiones entrantes de clientes SMB.Esta configuración está almacenada en en el registro:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\RequireSecuritySignature. Si esta configuración está activada, el servidor requiere que todo el tráfico SMB sea firmado. Si se lo desactiva, la configuración "EnableSecuritySignature" en el servicio del sistema guía el comportamiento del Server.

Las primeras dos configuraciones, aquellas que comienzan con Microsoft Network Client, afectan al servicio del Workstation. Los últimos dos, que comienzan con Microsoft Network Server, afectan el servicio del servidor. Éste es un punto críticamente importante:

Las configuraciones no tienen nada que ver con que si el sistema esté actuando primariamente como servidor o cliente en la red. Todos los sistemas tienen ambos un servicio de Workstation y de Server. Eso significa que ambas configuraciones afectan a todos los sistemas basados en Windows y Ud. necesitará considerar cuidadosamente cómo interactúan. Por lo tanto, usaremos de aquí en adelante el término "server" para referirnos a la máquina que está actuando como cliente en la misma transacción.

Las configuraciones por defecto para cada una de éstos son relativamente sencillas:

- El servicio de Workstation está configurado para habilitar la firma en todos los Windows 2000 y superiores.
- El servicio de Server está configurado para deshabilitar la firma en todos los Windows 2000 y superiores.
- Los DCs Windows 2000 están configurados para habilitar la firma en el servicio del servidor.
- Windows Server 2003 DCs están configurados para requerir la firma en el servicio del servidor.
- Windows 9x no soporta firma de mensajes de SMB, como tampoco lo hacen varios clientes y servidores de SMB de terceros.

La interacción entre estas configuraciones es bastante engañosa. Si el "servicio de servidor" en el servidor, por ejemplo, está configurado para requerir la firma ("Microsoft Network Server: Firma digitalmente las comunicaciones (siempre)" activado), el servicio del Workstation debe tener habilitada la firma o la comunicación fallará. La s tabla 1 muestra la interacción entre las configuraciones en el Server y en el cliente:

SERVICIOS SERVIDOR	SERVICIOS DE LA WORKSTATION		
	DESHABILITADO	HABILITADO	REQUERIDO
DESHABILITADO	Sin Firmar	Sin Firmar	Fallo en Conexión
HABILITADO	Sin Firmar	Datos Firmados	Datos Firmados
REQUERIDO	Fallo en Conexión	Datos Firmados	Datos Firmados

Tabla 1 Interacciones de firmas de mensajes del SMB

Cómo disparase un tiro por la culata

Está claro a esta altura que tenemos un problema. El Controlador de Dominios de Windows Server 2003 requiere la firma de mensajes, mientras que Windows 9x no lo soporta, así que una manera de dispararte en el pie es usar Windows 9x. Pero eso ya lo sabemos.

Si Ud. simplemente deja las configuraciones por defectos como vienen no debería tener problemas (exceptuando la anterior cuestión con Windows 9x). En lugar de eso, un montón de gente parece tener problemas con la firma de mensajes SMB. Claramente, la gente está cambiando las configuraciones por defecto. Una manera muy fácil de disparase en el pie es seguir todas las guías de seguridad disponibles que le dicen que debe requerir la firma de mensajes del SMB en el servicio del Workstation. Ésto en genral no puede causar problemas. Bloquea el ataque de reflejo al SMB. Desafortunadamente, a menos que Ud. habilite la firma de mensajes del SMB en todos los servidores a la vez, también te pone en la casilla "Workstation/Requerido - Server/Deshabilitado" en el recuadro de más arriba, en donde todas las conexiones fallan. Mucha gente falla en darse cuenta de que si simplemente requieren firmar en el cliente, éste ya no puede hablar a ningún servidor configurado con los valores por defectos. Ésta es la primer manera en la que la gente se disparan a sí mismas con esta configuración.

La segunda manera ocurre una vez que se dan cuenta de que no pueden conectar sus servidores. Como no hay manera fácil de volver a las configuraciones por defectos, parece que mucha gente desactiva la firma de mensajes en el servicio de Workstation. Ésto restaura la conectividad a los servidores, pero rompe la conectividad con el Controlador de Dominios (Domain Controller, DC) de Windows Server 2003, ya que esto requieren que se firmen los datos.

De hecho, hace que un cliente moderno actúe como un sistema Windows 9x, el cual tampoco soporta la firma por defecto y por lo tanto no puede hablar con el DC Windows Server 2003. Para trabajar apropiadamente con el DC de Windows Server 2003, todo los clientes deben soportar y tener habilitado la firma de mensajes de SMB. En otras palabras, tiene que tener por lo menos la configuración "Microsoft network client: Digitally sign communications (if server agrees)" activada.

Tercera, una realmente fácil manera de dispararse a uno mismo es deshabilitar la firma de mensajes del SMB. Dicha firma, mitiga serias cuestiones de seguridad validando todos los paquetes en un intercambio SMB. Es cierto que podría usar IPsec (Internet Protocol security) sobre SMB para alcanzar un efecto similar, pero a diferencia de la firma de mensajes SMB, IPsec no detiene ataques. Simplemente se asegura de que sólo seamos atacados por gente que conocemos. La firma de mensajes de SMB frena del todo los ataques. Por lo tanto recomendamos altamente la activación de la misma para tráfico crítico como el del controlador de dominios.

Activar la firma de mensajes, de hecho nos lleva a la razón por la que está deshabilitada en los servers por defecto, y a la última de las maneras de que nos salga el tiro por la culata al configurar la seguridad. La activación de la firma de mensajes del SMB modifica la forma en cómo son transmitidos los datos. Ésto significa que la carga de datos adicional será insignificante en transacciones pequeñas, como transferir archivos sin mucho tamaño. Sin embargo, para cada transferencia de archivos muy grandes, el peso de los datos que agregará la firma podría ser extremadamente alto (hasta un 40% en algunos casos). Por lo tanto tendrá que pensar dónde lo activará.

Claramente, la firma de mensajes de SMB tiene un significativo valor en materia de seguridad. Sin embargo, (como hemos discutido en el primer artículo de la serie de management de seguridad), este valor trae un costo; en este caso, en materia de performance, pero también en compatibilidad. Nadie puede decirle que "debería requerir la firma de mensajes del SMB en todos lados", sin antes hacer un detallado análisis de los riesgos. El costo puede ser significativo, pero el riesgo es que las credenciales de usuarios son robadas o retransmitidas contra un servidor más luego. Si el riego supera el coste de la activación de este sistema, debería requerir su activación en todos lados. Ni yo ni nadie puede decirle que tiene que hacerlo, a menos que hagan el análisis. Hacia lo que apunta este artículo es darle la información que necesita para tomar una decisión inteligente, y ayudarlo a evitar que le salga el tiro por la culata por una configuración incorrecta. ■

Este artículo también apareció en "Microsoft Security Newsletter, Vol. 2 Issue 9" (Gratuito) al que recomendamos suscribirse.

FIRMA DIGITAL

Ezequiel Eduardo Pawelko
Licenciado en Sistemas de Seguridad en Telecomunicaciones
Ingeniero en Telecomunicaciones

¿Qué es una Firma digital?
Wikipedia (www.wikipedia.org) nos aclara: "Firma digital (digital signature) o "firma digital de llave pública", es un tipo de método de autenticación para información digital, análoga a las firmas físicas comunes realizadas en papel. Su implementación se realiza usando técnicas del campo de la criptografía de llave pública. Un método de firma digital, usualmente define dos algoritmos complementarios, uno para firmar y el otro para verificación. El resultado del proceso de firmado es también llamado "firma digital"".

El término"Firma digital" ha sido también utilizado en un contexto más amplio abarcando las llamadas firmas digitales de llave pública y los códigos de autenticación de mensajes (Message Autentication Codes (MAC).

Las firmas digitales difieren de algún modo de sus contrapartes físicas. El término firma electrónica, usado algunas veces para la misma cosa, tiene un significado diferente bajo la ley. Se refiere a uno de varios mecanismos, no necesariamente criptográficos, que permiten identificar quién envía un mensaje electrónico. Firmas electrónicas han incluido telegramas, telex y transmisión por fax de firmas manuscritas sobre un documento de papel.

Cuando hablamos de Firma Digital siempre utilizamos términos de las técnicas criptográficas y, en ocasiones, estas aplicaciones pueden llevar a confusiones. Para aclarar los conceptos que encierra el sistema de Firma Digital consideremos brevemente su evolución.

Los sistemas criptográficos nacen siendo sistemas de claves secretas (también llamadas compartidas o de de sesión). Estos sistemas usan una única clave para cifrar y/o descifrar la información en el emisor y receptor del mensaje, respectivamente. (Fig.1)

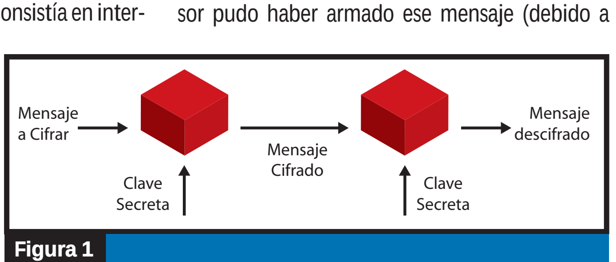
Dichos sistemas criptográficos tienen por objeto convertir a un canal de comunicaciones inseguro en un canal de comunicaciones seguro, al hacer que la información que viaje por él sea ilegible para todo aquel que la pueda interceptar y que no posea la clave secreta para descifrar el mensaje. Este tipo de sistema es usado desde los inicios de la criptografía, donde el sistema consistía en intercambiar cada letra del abecedario, hasta los complejos algoritmos matemáticos que sólo pueden ser procesados con los potentes computadores que hoy tenemos, en tiempos razonables.

Siendo un poco más técnico, desde el punto de vista de la seguridad, todo el sistema de clave secreta ofrece:

1. Confidencialidad: se refiere al hecho de que la información no ha sido "vista" por otras personas mientras viaja por el canal de comunicaciones desde el emisor al receptor.
2. Integridad: esta condición describe el hecho de que la información cifrada que llega al receptor no ha sido alterada durante su viaje a través del canal de comunicaciones.

Estas dos condiciones son fundamentales para mantener la privacidad de la información.

Si el sistema de clave secreta sólo posee dos usuarios, cada uno de ellos podrá afirmar que el mensaje recibido es enviado por el otro usuario ya que éste puede descifrarlo utilizando la clave privada que ha usado el emisor para enviarle el mensaje. Si suponemos fehacientemente que sólo el emisor pudo haber armado ese mensaje (debido a



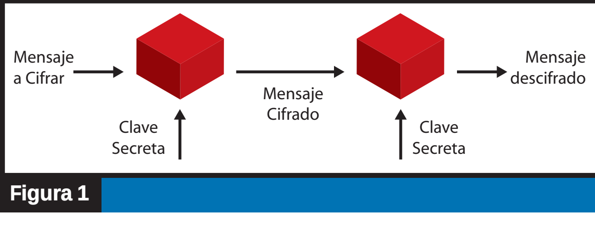


Figura 1



que sólo él tiene la clave secreta) estamos realizando una "autenticación". La autenticación es una tercera condición que describe el hecho de que se pueda garantizar que una determinada persona (y solamente ella) sea la que ha realizado la operación de cifrado y envío del mensaje.

La autenticación es el requisito básico de un sistema de firmado. Cuando nosotros firmamos algo en forma manuscrita, dicha firma nos autentica, ya que sólo un tipo de firma puede ser realizada por una persona. (Fig.2)

Si el sistema estuviera compuesto por tres usuarios A, B y C, donde cada uno de ellos se puede comunicar con los otros de manera segura (todos tienen la misma clave), todo mensaje que llega al usuario "C" no se podría determinar por medio del sistema criptográfico si provino de "A" o de "B".

En conclusión, un sistema de claves secretas sólo puede dar autenticación si el sistema encierra sólo dos usuarios y se puede garantizar que sólo ellos conocen la clave y que nadie puede falsificar un mensaje cifrado proveniente de alguno de ellos.

Como hemos comentado anteriormente, el sistema de clave secreta, cumpliendo con los requisitos anteriores, permite dar autenticación y ésta es el requisito indispensable para crear un sistema de Firma Digital. Sin embargo, esto no se aplica en la práctica porque esta técnica es impractica si el sistema alcanza a varias personas. Consideremos qué sucede si queremos que muchas personas se autentiquen entre ellas:

Como vimos hasta ahora, para garantizar autenticación se tiene que cumplir el requisito de que la clave secreta la conozca solamente el emisor y el receptor del mensaje, los cuales, cuando lo deseen, pueden invertir su papel a receptor y emisor, respectivamente.

Si el sistema tiene dos personas, cada una deberá recordar sólo una clave. Si el sistema está integrado por tres personas, cada una deberá recordar dos claves. Si el sistema es de cuatro, cinco o seis personas, cada una de ellas deberá recordar seis, diez y quince claves, respectivamente. Si bien parecen pocas las claves, el sistema se vuelve cada vez más complejo a medida que aumenta el número de usuarios. Si el sistema tuviera mil usuarios, cada uno debería recordar 499.500 claves secretas. (Fig. 3 y 4)

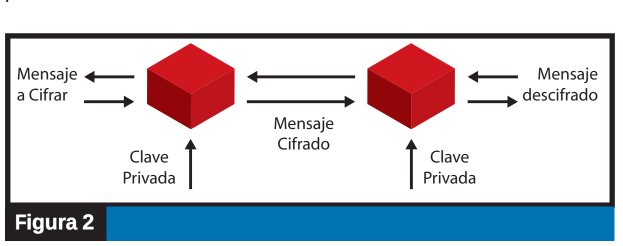


Figura 2

La desventaja principal del sistema al utilizarse a tal escala radica principalmente en que sería imposible garantizar que cada uno de los mil usuarios proteja debidamente la confidencialidad de las claves que tengan en su poder, además de complicarse la administración de las claves que debe ser realizada por una autoridad centralizada.

Por las razones hasta aquí analizadas es que se ha utilizado un sistema criptográfico denominado "de clave pública" o "asimétrico" y no el simétrico o de clave secreta. La palabra "asimétrico" radica en que este sistema, a diferencia del sistema de clave secreta, utiliza dos claves: una pública y otra privada. La clave privada sólo es conocida por una sola persona y la clave pública es publicada o difundida sin que esto altere las características del sistema.

Los sistemas asimétricos son extremadamente modernos, ya que sus algoritmos matemáticos sólo son posibles de procesar, en períodos razonables desde el nacimiento de las computadoras.

Clave criptográfica privada: En un criptosistema asimétrico es aquella que se utiliza para firmar digitalmente.

Estos algoritmos o sistemas asimétricos fueron diseñados inicialmente para trabajar en la configuración mostrada en la Figura 5.

El usuario B publica su clave pública con el objeto de que las personas le envíen mensajes cifrados con su clave pública. El usuario A cifra un mensaje utilizando el algoritmo asimétrico y la clave pública para luego enviar el mensaje cifrado al usuario B. En esta configuración, el mensaje cifrado con la clave pública B sólo puede ser descifrado con la clave privada de B (que sólo el usuario B conoce). Por lo tanto, en esta implementación cada usuario difunde su clave y mantiene en secreto su clave privada. Este sistema da confidencialidad, porque nadie más que el que posee la clave privada del mensaje cifrado puede descifrarlo, además de integri-

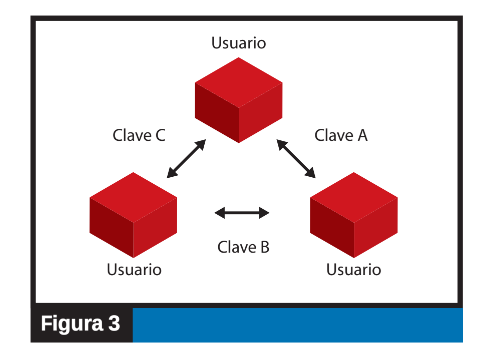


Figura 3

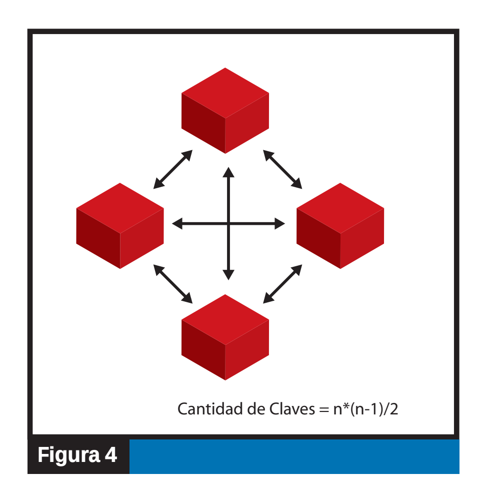


Figura 4

dad, ya que, si la información es modificada, el usuario receptor no podrá descifrarla o se dará cuenta de la alteración, pero no garantiza autenticación por lo que no se lo puede usar en el sistema de Firma Digital.
La otra configuración a realizarse con el sistema

Clave criptográfica pública: En un criptosistema asimétrico es aquella que se utiliza para verificar una firma digital.

de criptografía de clave pública es la que se utiliza en el sistema de Firma Digital. La configuración es la que se ve en la figura 6.
En esta arquitectura, el emisor también difunde su clave pública y protege su clave privada como el de la anterior configuración, pero con la diferencia de que ahora cifra el mensaje con la clave privada. Esta configuración permite que cualquier usuario del sistema que tenga la clave pública del otro usuario pueda descifrar los mensajes cifrados por este.
A diferencia de la primera configuración, que garantizaba confidencialidad e integridad de la información, esta configuración otorga garantías de integridad y de autenticación. Cabe aclarar que los sistemas de Firma Digital propiamente dichos no garantizan confidencialidad de la información firmada, por lo que para mantener su privacidad debe utilizarse algún otro sistema de criptografía ya sea simétrico o asimétrico. (Ver Cuadro)
Lo anterior se debe a que el documento a firmar en realidad se trasmite de forma legible, lo que se cifra es en realidad un hash del documento original por lo que el documento digital viaja con la firma "adjunta". En estas condiciones cualquier persona puede leer el mensaje y solo comprueba la autenticidad de la firma cuando lo desee.
En la práctica el sistema de Firma Digital consiste en toda una arquitectura que según la ley se denomina Infraestructura de Firma Digital la cual define no solo a los usuarios sino también a las entidades encargadas de garantizar la autenticidad de las firmas de los usuarios como así también de entes que controlan a estos últimos.
Para poder difundir correctamente las claves publicas de los usuarios, se difunden certificados denominados certificados digitales, y que cuya función es vincular los datos del usuario con los de la Firma Digital.

Panorama Legal de la Firma Digital

Como se ha comentado, la Firma Digital tiene por objeto autenticar al firmante de un documento digital. Existen muchas aplicaciones que permiten crear firmas digitales (como PGP) y de empresas que se encargan de garantizar la confiabilidad del sistema de firmas a los usuarios, pero que sus firmas no tienen necesariamente validez legal.
La Firma Digital nace en el ámbito de Internet, impulsada por el comercio electrónico que mueve billones de dólares al año. Para que el comercio tenga un mayor dinamismo se requiere que se puedan firmar contratos con validez legal a través de Internet. Si bien se puede utilizar PGP para autenticar a alguien, firmar un contrato o un documento con este método no es considerado un contrato con validez legal, ya que la Firma Digital utilizada no reemplaza la firma manuscrita que exige la ley, por lo que la justicia se de-sentiende de la validez del contrato. Lo que se requiere es que se le de validez legal a la Firma Digital para que pueda ser utilizada en los lugares donde clásicamente se utiliza la firma manuscrita y esto es lo que hace Ley de Firma Digital.
Nuestro país en el año 2001 ha creado la Ley de Firma Digital (Ley Nº 25.506) con el objetivo de desarrollar una infraestructura que de validez jurídica a la Firma Digital, de manera que se la pueda emplear en todos aquellos lugares donde se exija una firma manuscrita.
La creación de una ley de estas características en nuestro país no es poco debido a lo difícil que es regular la Red de Redes, Internet. Según ha definido la Secretaria de Comunicaciones (o SECOM, organismo estatal encargado de regular las Telecomunicaciones y la Sociedad de la Información en la Argentina), Internet se comprende como una red de alcance mundial cuyo crecimiento exponencial se debe a su naturaleza de autorregulación, por lo cual su reglamentación debe ser mínima. En este contexto, la Secretaria de Comunicaciones ha hecho referencia a un fallo de la Corte Suprema de justicia de los Estados Unidos que ha determinado que Internet es una especie de comunicación privada de alcance mundial y como tal su reglamentación es nula o mínima.
La Ley define a la Firma Digital como el resultado de aplicar a un documento digital un procedimiento matemático que re-quiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La Ley también exige que la información de cifrado se encuentre bajo absoluto control del dueño ya que de está depende la confiabilidad del sistema. Si un usuario descuida su firma, entonces cualquier persona se puede hacer pasar por él en cuestiones de carácter legal, llevando al degradamiento del sistema.

Mensaje a Cifrar
Mensaje Cifrado
Mensaje descifrado
Clave Privada
Clave Privada

Figura 5

Se aprecia que el sistema será confiable en la medida en que los usuarios mantengan el compromiso de guardar en absoluto secreto su firma.
El articulo dos de la Ley también habla de que el sistema a implementarse debe garantizar la integridad de la información y la autenticación de la persona firmante, al respecto dice: "La Firma Digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma".
En el artículo anterior aparece un nuevo concepto jurídico denominado técnicamente NO REPUDIO. El no repudio consiste en no poder negar que quien firmo un documento digital no lo haya hecho. El no repudio puede entenderse como una autenticación con validez legal, por lo cual diremos que solo un sistema de Firma Digital aprobado legalmente tiene la característica de no repudio. En este contexto decimos que si bien PGP tiene las mismas características que un sistema de firma legal, no cumple con la condición de no repudio.
La Ley de Firma Digital para su implementación define cuidadosamente ciertos conceptos que hacen a la Infraestructura de Firma Digital:
Firma electrónica. Es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que

Sistema	Cifrado	Descifrado	Garantía
PKI (asimétrico)	Pública	Privada	Confidencialidad - Integridad
PKI (asimétrico)	Privada	Pública	Integridad - Autenticación
PKI (Firma Digital según Ley)	Privada	Pública	Integridad - No repudio (autenticación Legal)
Simétrico (clave Privada)	Privada	Privada	Confidencialidad - Integridad

Cuadro


La Certificación más prestigiosa en Seguridad Informática
CentralTECH te invita a participar de la Carrera de Certificación
CISSP
Certified Information Systems Security Professional
Próximos inicios Marzo y Abril 2006
Seminarios Informativos
www.centraltech.com.ar/seminarios,
Comuníquese al (011) 5031-2233,
masinfo@centraltech.com.ar, o personalmente en:
Av. Corrientes 531, 1° piso
Capital Federal - Buenos Aires
Argentina
CentralTECH
Capacitación Premiere
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
(CISSP)
FOTO: (c) JUPITERIMAGES, and its Licensors. All Rights Reserved

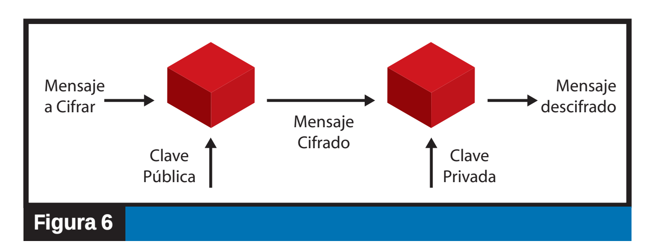
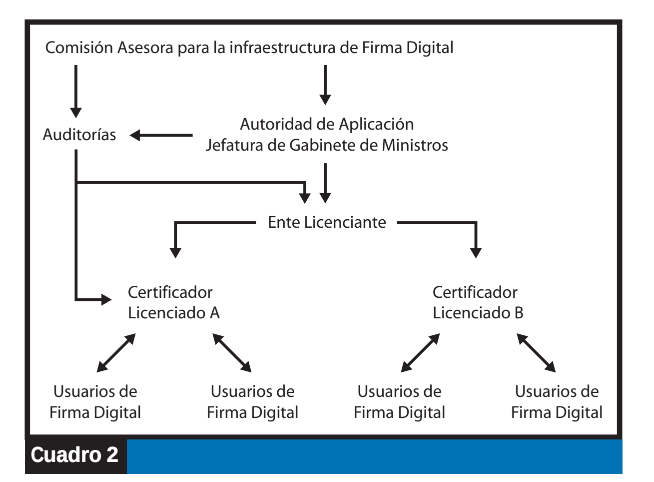


Figura 6

carezca de alguno de los requisitos legales para ser considerada Firma Digital.
En el contexto de la firma electrónica podemos encontrar que el mail puede ser considerado como Firma Electrónica pero no como Firma Digital. La consideración del correo electrónico en nuestra legislación es muy importante y recibe una definición jurisprudencial, es decir en base a la opinión de los jueces. El mail tal como lo conocemos no esta definido en la Ley de Telecomunicaciones (Ley Nº 19798 del 72, Ley que regula el aspecto técnico de las Teleco-municaciones en nuestro país) pero por jurisprudencia se ha determinado que es, al igual que un mensaje, una correspondencia de telecomunicaciones y desde entonces su validez legal.

Criptosistema asimétrico: Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha firma digital.

Documento digital. El documento digital es toda representación digital, con independencia del soporte físico utilizado para su fijación, almacenamiento o archivo.
La definición del documento digital satisface plenamente el requerimiento de escritura de forma análoga a como lo hace la Firma Digital con la manuscrita.
Certificado digital. El certificado digital es un documento digital firmado digitalmente por un certificador (entidad encargada de garantizar la autenticidad de una Firma Digital) y cuyo objetivo es el de vincular los datos de verificación de firma a su titular.
Estos certificados tienen periodo de vigencia para que el sistema sea seguro y confiable.
La Unión Internacional de Tele-comunicaciones (ITU), que es el organismo internacional idóneo en la materia de Telecomunica-ciones y de la Sociedad de la Información, es el encargado de generar las recomendaciones de los Certificados Digitales que utilizamos.
Certificador Licenciado: Es un ente autorizado por el Estado a emitir certificados digitales.
Los certificadores licenciado pueden ser personas de existencia real, organismos públicos o consejos de profesionales que controlen matriculas. La Ley da a estos certificadores las siguientes funciones:
• Emitir los certificados Digitales.
• Identificar los Certificados Digi-tales emitidos por él.
• Mantener copia de todos los certificados digitales emitidos por él.
Si bien la Ley y su decreto reglamentario han aparecido hace tiempo, el sistema no se encuentra aun habilitado a nivel nacional ya que los Certificadores Licenciados solo han aparecido a nivel de organismos públicos, para uso interno, como en los consejos profesionales para el control de los matriculados solamente. Recientemente el COPITEC (Consejo Profesional de Ingeniería en Telecomunicaciones, Electrónica y Computación) ha comenzado a funcionar como Certificador para sus matriculados.
(www.copitec.org.ar)
Ente Licenciante: Es la autoridad que autoriza o licencia a los Certificadores Licenciados para que cumplan tal función. Esta formado por una comisión controlada a su vez por la jefatura de Gabinete de Ministros quien es la Autoridad de aplicación de la Ley de Firma Digital. (Fig.7)
Comisión Asesora para la Infraestructura de Firma Digital: Se trata de una comisión de asesoramiento integrada multidisciplinariamente por un máximo de siete profesionales de carreras vinculadas con la actividad informática de reconocida trayectoria y experiencia, provenientes de Organismos del Estado nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de profesionales.
La Comisión emite recomendaciones a la autoridad de aplicación sobre:
• Estándares tecnológicos;
• Sistema de registro de toda la información relativa a la emisión de certificados digitales;
• Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;
•Metodología y requerimiento del resguardo físico de la información, etc.
Sistema de Auditoria. La autoridad de aplicación y la Comisión Asesora para la Infraestructura de Firma Digital diseñan sistemas de auditoria para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, como así también los planes de seguridad y de contingencia aprobados por el ente licenciante.
Recordemos que el sistema es confiable si los usuarios del mismo son capaces de mantener en absoluto secreto y bien resguardado su sistema de cifrado con su clave, por lo que la Ley exige a los titulares de certificados digitales una serie de cuestiones como:
• Mantener el control exclusivo de sus datos de creación de Firma Digital, no compartirlos, e impedir su divulgación;
• Utilizar un dispositivo de creación de Firma Digital técnicamente confiable;
• Solicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
• Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.



Cuadro 2

Nuestro modelo de ley de Firma Digital que hemos tomado ya fue implementado en mucho s países. La idea detrás de esto es hacer que la Firma Digital tenga un alcance internacional siempre y cuando existan acuerdos de reciprocidad entre los países. En este contexto, si un ciudadano español firma un documento en España utilizando un Certificador Licenciado por el gobierno de España, su firma tendrá validez en nuestro país si existen acuerdos entre ambos países.
En resumen, la Firma Digital implica mecanismos de verificación de integridad de la información y de autenticación del firmante, llamada legalmente no repudio, con el objeto de poder utilizar este tipo de firma en reemplazo de la firma manuscrita. ■

Mensaje
a Cifrar
Mensaje
Cifrado
Mensaje
descifrado
Clave
Privada
Clave
Pública

Figura 7



Instalación de software bajo Linux

Pablo González Mateos
Licenciado en Sistemas de Información

En sistemas operativos Open Source como Linux, son múltiples las opciones a la hora de elegir la forma en que un administrador instala software, ya sea de aplicación o de servicios en el sistema, siendo posible utilizar diferentes formatos binarios o bien, comenzar desde cero, compilando desde codigo fuente!

INTRODUCCION

Sistemas de paquetes RPM

Red Hat introdujo en el mundo de sistemas Linux un formato de paquetes de software que permite que la instalación de software sea relativamente simple. El RedHat Packet Management consiste básicamente en un conjunto de herramientas, que, con la ayuda del comando "rpm", se encargan de las tareas de descomprimir un programa, instalarlo, e instalar las librerías y archivos de configuración en los directorios que fuera necesario. Su funcionamiento es bastante simple, y consiste en que el usuario debe conseguir el archivo .rpm del software que desea instalar, depositarlo en algún directorio y finalmente ejecutar el siguiente comando:

```
rpm -ivh nombre-archivo.rpm
```

El principal problema de este sistema ocurre cuando el software a instalar requiere que previamente esté instalado en el sistema algún otro paquete, librerías o algún archivo determinado. Esta situación se denomina "problema de dependencias de software". Para remediarlo hay que navegar en Internet, buscar el paquete que contiene el software necesario, instalarlo y posteriormente instalar el paquete inicial. Esta situación puede volverse un poco compleja si los paquetes a instalar son complejos a nivel de dependencias.

Para consultar la base de datos rpm (el listado completo del software instalado en el sistema), se puede utilizar el siguiente comando:

```
rpm -qa
```

Probablemente se genere un listado enorme de paquetes, por lo que si uno necesita ver si un determinado paquete se encuentra instalado, podemos hacer uso del filtro “grep” de la siguiente forma:

```
rpm -qa | grep paquete-a-buscar
```

Sencillamente, si el sistema responde con el prompt, la respuesta es que el paquete no se encuentra instalado, de lo contrario devolvera el o los paquetes que satisfacen el criterio de busqueda y los números de versión de los mismos.

Sistemas de paquetes apt

Este sistema de paquetes es impulsado principalmente por la distribución Debian GNU/Linux, y consiste en un conjunto de herramientas que permiten automatizar la instalación de software y resolver los conflictos de dependencias habituales con los sistemas *rpms*. La configuración básica del “apt” puede realizarse desde un comando interactivo llamado apt-setup. Una vez configuradas las fuentes de descarga de software sólo resta instalar lo que necesitemos via apt-get (Figura 1).

El apt-get se encargó de conectarse por medio de un ftp a un repositorio, descargar la versión correspondiente del "mc", (habiendo calculado previamente las dependencias) y finalmente se encargó, mediante un llamado al programa “dpkg”, de instalar el paquete correspondiente. En el ejemplo el software instalado es un clon del Norton Commander, (un popular gestor de archivos para DOS), llamado Midnight Commander. Para invocarlo basta con tipear en la consola:

```
mail:~# mc
```

Desde “apt” es muy sencillo mantener el software actualizado, el siguiente comando compara cada uno de los paquetes instalados en el sistema y se ocupa de chequear contra el repositorio de software si existen versiones nuevas de los mismos, en cuyo caso automáticamente las descarga e instala. Fácil, no ?.

```
mail:~# apt-get upgrade
```

INSTALACION DE SOFTWARE DESDE CODIGO FUENTE

El porqué de esta metodología

Esta metodología es quizás la menos práctica, menos ordenada y por que no la más complicada y lenta. Entonces, por qué uno decidiría instalar software de esta manera? Bien, creo que encontramos múltiples respuestas a esta pregunta, que hacen justificable esta forma de trabajo; veamos algunas de ellas:

Seguridad: Cuando un desarrollador compila un software, no sabe cuál va a ser la plataforma o el uso que se le va a dar al mismo, por lo tanto no tiene más opción que compilar el software con todos sus componentes. En caso de un software de servicios (como puede ser un servidor de páginas web), ésto involucra seguramente a funcionalidades y librerías que probablemente el usuario no vaya a utilizar nunca. En el caso particular del software de servicios, existe la posibilidad de que un error de codificación del software sea explotado por un atacante remoto, para obtener recursos en el servidor, como por ejemplo un shell. Si uno reduce el binario del servidor, incluyendo sólo las funcionalidades a ser utilizadas, se reduce en gran parte la probabilidad de que el sofware contenga un fallo de seguridad explotable.

Performance: Es posible al compilar el software, indicar al compilador que optimice el código fuente para la plataforma en la que se ejecutará. En la mayoría de las distribuciones Linux modernas, el software empaquetado viene compilado para procesadores x486 o superiores, de forma que no se hace un uso directo de instrucciones de procesadores más modernos como pueden ser Athlon, Pentium 4, etc. Al quitar componentes o módulos que no serán utilizados, se logra un binario de menor tamaño, que consume menos memoria y se ejecuta mas rápido.

Disponibilidad multiplataforma: No siempre encontramos en nuestra distribución favorita un paquete binario (compilado para nuestra plataforma) disponible para instalar. Si bien distribuciones como Debian incluyen más de 15.000 aplicaciones, no es tan extraño necesitar de un software que no esté dentro del repositorio oficial. Por lo que una opción para obtener ese software sería instalar desde código fuente.

Los repositorios de software libre

Existen en Internet innumerables sitios que se dedicar a publicar software bajo algún tipo de licencia Open Source (GPL, LGPL, BSD, etc). Sin

Figura 1:

```
mail:~# apt-get install mc
Reading Package Lists... Done
Building Dependency Tree... Done
Suggested packages:
  zip
The following NEW packages will be installed:
  mc
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 2155kB of archives.
After unpacking 5328kB of additional disk space will be used.
Get:1 http://ftp.es.debian.org testing/main mc 1:4.6.0-4.6.1-pre3-3  [2155kB]
Fetched 2155kB in 27s (78.1kB/s)
Selecting previously deselected package mc.
(Reading database ... 45570 files and directories currently installed.)
Unpacking mc (from .../mc_1%3a4.6.0-4.6.1-pre3-3_i386.deb) ...
Setting up mc (4.6.0-4.6.1-pre3-3) ...
Installing new version of config file /etc/mc/mc.menu ...
Installing new version of config file /etc/mc/mc.ext ...
mail:~#
```

Figura 2:

```
storage:~# cd /usr/local/src/
storage:/usr/local/src# wget        http://freshmeat.net/redir/seatris/9370/url_tgz/seatris-0.0.14.tar.gz
--13:45:59--  http://freshmeat.net/redir/seatris/9370/url_tgz/seatris-       0.0.14.tar.gz
            => `seatris-0.0.14.tar.gz.1'
Resolving freshmeat.net... 66.35.250.168
Connecting to freshmeat.net[66.35.250.168]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 53,056 [application/x-tar]
           100%[====================================>] 53,056        36.36K/s
           13:46:02 (36.31 KB/s) - `seatris-0.0.14.tar.gz' saved [53056/53056]
```

embargo prácticamente todo el software libre podemos encontrarlo en los siguientes sitios:

http://www.freshmeat.net
http://www.sourceforge.net
http://www.gnu.org

Descargando un software

Navegando por freshmeat.net encontramos un software que nos puede servir de ejemplo de compilación, y a la vez quizás nos divirtamos un poco, después de todo nadie puede dedicarse al trabajo el 100% de su tiempo, no? El software elegido sea llama "Seatris", y es un clon del popular Tetris para consola, sí, sin necesidad de tener Xwindows! Comencemos con la instalación (figura 2.)

Hasta aquí lo que hemos hecho es cambiarnos al directorio /usr/local/src. Este directorio es un buen lugar donde depositar todo aquel software que se instale por esta metodología, con el objetivo de no dispersar archivos sobre el nivel del directorio /usr/local. Luego con el comando "wget" pasando como argumento la URL del archivo y obtenemos el código fuente en "seatris-0.0.14.tar.gz".

Descomprimiendo y desempaquetando

Si el archivo a descomprimir tiene extensión .tar.gz, nos indica que está empaquetado con el comando "tar" y comprimido con el "gunzip". Para desempaquetar y descomprimir el software utilizamos el siguiente comando:

storage:/usr/local/src# tar -xzvf seatris-0.0.14.tar.gz

Nota: Si la extensión del archivo hubiera sido .tar.bz2, entonces será necesario tener instalado el bzip2 (otro compresor/descompresor mas potente), y el comando tar debería invocarse con las opciones "tar -xjvf archivo.tar.bz2".

Ahora, veremos que se ha creado un directorio llamado seatris-0.0.14; ingresemos al directorio:

storage:/usr/local/src# cd seatris-0.0.14

Ahora sí a compilar!!!

Bueno, en realidad no tan rápido, primero debemos ejecutar un script que controlará si tenemos en nuestro sistema las librerías necesarias para compilar el seatris. Este script ya viene preparado y se llama "configure" (Figura 3)

Error !!! Bueno, a no desesperarse, ésto es cosa de todos los días para un administrador Unix que compila software. Veamos que sucedió en la última línea del "configure":

checking for ncurses header file... configure: error: not found

Este mensaje nos indica que el seatris necesita de las bibliotecas ncurses (que son las que permiten compilar software para consola con soporte a dibujar pantallas bajo la consola. Bien debemos entonces instalar la librería ncurses-dev. En este caso lo haremos con Debian, en un sistema con rpms habría que descargar el .rpm e instalarlo manualmente:

storage:/usr/local/src/seatris-0.0.14# apt-get install ncurses-dev

Bien, veamos qué sucede ahora que tenemos la librería instalada, volviendo a ejecutar el script "configure":

storage:/usr/local/src/seatris-0.0.14# ./configure
....
creating Makefile
creating autoconf.h

Bárbaro, el script pudo finalizar su ejecución y creó un archivo llamado Makefile, el cual contendrá información para que el compilador sepa con que parámetros deberá compilar el software. Ahora debemos ejecutar el comando "make" para compilar.

storage:/usr/local/src/seatris-0.0.14# make

Si no hubo mensajes de error, significa que el software se compiló correctamente. Ahora ejecutaremos un comando que copiará los binarios, la documentación, y la configuración del Seatris a los directorios que corresponda. (siempre dentro de nuestro /usr/local) (Figura 4.). Vemos que el binario ha quedado instalado en el directorio /usr/local/games, ejecutémoslo a ver que pasa:

storage:/usr/local/src/seatris-0.0.14# /usr/local/games/seatris

Enhorabuena !!! Despues de tanto trabajo merecíamos un poco de diversión, no?

Recomendaciones para tener un sistema capaz de compilar

Normalmente necesitamos un conjunto de herramientas básicas instaladas en nuestro sistema, como para poder compilar, he aquí un conjunto de paquetes que deberían estar instalados: gcc, g++, make, autoconf, glibc.

Nota

¿Por qué "./configure" y no sólo "configure" ?. La respuesta es sencilla: Un sistema Linux, por cuestiones de seguridad, no intenta ejecutar ningún programa que no este listado dentro de la variable de entorno "PATH". Es seguro que en nuestro caso, el directorio /usr/local/src/seatris-0.0.14 no estaba declarado en el PATH, ya que acabamos de crear el directorio!, por lo tanto la opción mas cómoda es ingresar al subdirectorio "seatris-0.0.14" e invocar al script ./configure, donde el "./" simboliza el directorio actual, de manera que el shell sepa la ruta exacta del ejecutable. Si uno quisiera, también podría invocarlo en forma absoluta: "/usr/local/src/seatris-0.0.14/configure", pero por lo general no queremos tipear tanto.

De yapa

Para los amantes del máximo aprovechamiento de recursos, existe una excelente distribución Linux que se basa en la filosofía de compilar absolutamente todo el software. Para ello tiene un sistema de instalación de software basado en árboles de dependencias de código fuente muy potente, llamado "emerge", donde para compilar e instalar un software sólo hace falta tipear un comando como el ejemplo:

emerge mc

El sistema se encarga de controlar las dependencias, bajarlas y compilarlas una por una hasta llegar a tener el software indicado listo para usar.

En síntesis

Hemos aprendido las diferentes metodologías de instalación de software bajo Linux, como binarios .rpm, sistema apt estilo Debian, e incluso compilar software desde codigo fuente. Trabajamos sobre un software que si bien es sólo un simple juego, nos permite aprender la metodología estandar de compilación. También experimentamos que pueden ocurrir inconvenientes, como la falta de alguna librería, y cómo solucionarlos. Esta metodología es prácticamente la misma para cualquier tipo de software que se quiera instalar bajo Linux, así que ahora a navegar por freshmeat.net y a compilar!.

Algunos links útiles

http://www.rpmseek.com
http://www.rpmfind.net
http://www.debian.org/distrib/packages
http://www.gentoo.org

Figura 3:

```
storage:/usr/local/src/seatris-0.0.14# ./configure
loading cache ./config.cache
checking for gcc... gcc
checking whether the C compiler (gcc  ) works... yes
checking whether the C compiler (gcc  ) is a cross-compiler... no
checking whether we are using GNU C... yes
checking whether gcc accepts -g... yes
checking for a BSD compatible install... /usr/bin/install -c
checking for ncurses header file... configure: error: not found
```

Figura 4:

```
storage:/usr/local/src/seatris-0.0.14# make install
install -o root -g games -m 2711 seatris /usr/local/games
touch /var/lib/games/seatris.score
chown root.games /var/lib/games/seatris.score
chmod 664 /var/lib/games/seatris.score
install -o root -g root -m 644 seatris.6 /usr/local/man/man6
```

BREVES

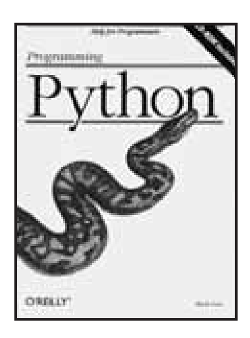
Cisco para llevar...



Según un reporte del Financial Times, Cisco Systems tiene en sus planes incursionar en el mercado masivo con productos hogareños.

Si bien no hay detalles específicos, Cisco quiere incorporar capacidad de networking en appliances de uso común como por ejemplo, radios que a parte de captar señales con base terrestre, también reproducirán streaming desde Internet. Este atrevido viraje estratégico de Cisco, puede deberse a que hoy sus acciones cuestan la quinta parte que hace 5 años, y a la necesaria adaptación a un mercado dinámico. En este sentido se realizaron la adquisición de Linksys en 2003 y recientemente de Scientific Atlanta. Si este cambio de target sucede, la gente deberá acostumbrarse a la presencia de Cisco en una góndola rodeado de fabricantes como Sony, Sharp o Sanyo.

Ya está disponible la primer versión Beta de IronPython.



La primer Beta del IronPython fue anunciada por Jim Huguini (desarrollador experto en lenguajes dinámicos de programación), quien fue contratado por Microsoft en 2004.
Dicha incorporación fue el 1° paso de la adquisición del lenguaje Python. Éste, es un lenguaje de scripting, de código abierto, creado por Huguini y desarrollado por la comunidad de programadores open source.
IronPython es parte de la iniciativa Shared Source de Microsoft, y consta de la integración del lenguaje original al .NET.

CTI Móvil invierte en infraestructura IP para ampliar su red en Argentina

CTI Movil realizó inversiones para mejorar su infraestructura de redes, migrar hacia tecnología IP y lograr una mejor convergencia de servicios de voz, video y datos.

Seleccionó la tecnología de Cisco Systems como la base estratégica para expandir los servicios de su red nacional y lograr la migración hacia una plataforma IP (Internet Protocol) con el objetivo de ampliar la capacidad de tráfico de llamadas y brindar nuevos servicios a través de la convergencia de voz, video y datos.
La tecnología implementada le permite a CTI estar mejor preparada para las demandas actuales y futuras del mercado. El nuevo backbone IP permite absorber hasta seis veces más del tráfico actual de llamadas y de servicios como transferencia de datos, mensajes SMS y servicios de 3° Generación.
Con las nuevas plataformas multiservicios y la solución IP-MPLS (Multiprotocol Label Switching) de Cisco Systems, CTI se ha convertirse en modelo a replicar por otras operadoras del grupo América Móvil en la región.
La solución adquirida por CTI Móvil está compuesta básicamente por plataformas multiservicio Cisco 7600 en el acceso de la red y equipos Cisco GSR12400 como equipamiento central de la red de alta capacidad IP-MPLS.
La implementación consistió en 3 etapas, al cabo de las cuales se extendió la cobertura del nuevo servicio a toda Argentina y Paraguay
La integración de este proyecto estuvo a cargo de la empresa Softnet Logical, Gold Partner certificado de Cisco Systems.





Las laptops de u$s 100 (aún no en producción), no estarán a la venta, sino que serán distribuidas a escuelas directamente a través grandes contratos gubernamentales.

El MIT Media Lab ha lanzado una nueva iniciativa para desarrollar una laptop por u$s 100. Es una tecnología que podría revolucionar cómo se educa a los chicos en el mundo. Para alcanzar esa meta, ha sido creada una nueva asociación sin fines de lucro: One Laptop per Child (OLPC). La iniciativa fue anunciada por primera vez en el Foro Económico Mundial en Davos, Suiza, en Enero de 2005 por el chairman del laboratorio y co-fundador, Nicolás Negroponte.
http://laptop.media.mit.edu

Humor - *Por Severi*

